MASTER EN SCIENCES INFORMATIQUES

L'identité numérique comme mécanisme de confiance pour l'économie collaborative

Brisbois, Laurent

Award date:
2021

Awarding institution:
Universite de Namur

Université de Namur
Faculté d'informatique
Année académique 2020–2021

L'identité numérique comme mécanisme de confiance pour l'économie collaborative

Laurent BRISBOIS

Promoteur : _____ (Signature pour approbation du dépôt - REE art. 40)
Claire LOBET

Mémoire présenté en vue de l'obtention du grade de
Master en Sciences Informatiques.

Abstract
L'économie collaborative est de plus en plus présente dans notre quotidien. Que ce soit par l'émergence de nouvelles plateformes qui tentent de se faire une place dans ce marché, ou tout simplement par l'engouement grandissant qu'il y a pour cette pratique qui consiste à s'échanger des biens ou des services entre particuliers. Nous sommes en effet de plus en plus nombreux à utiliser internet pour effectuer des transactions entre pairs (peer to peer). En parallèle à ce phénomène qui ne cesse de croître, la cybercriminalité, elle aussi, continue de sévir et les délits liés à l'identité se font de plus en plus nombreux. La particularité de l'économie collaborative est que dans la majorité des cas, nous faisons affaire avec de parfaits inconnus. Cela rajoute une dimension aux risques auxquels nous faisons face lors d'achats en ligne puisque, dans ce cas, notre interlocuteur n'est plus une entreprise ou une organisation mais bien un autre individu. Les plateformes qui supportent cette économie collaborative développent des mécanismes censés "rassurer" les utilisateurs. Mais ces mécanismes s'avèrent peu efficaces pour lever les incertitudes liées à ce type de pratique. Il importe donc de trouver des alternatives afin de construire une confiance plus "assurée" entre partenaires lors de transactions collaboratives. Pour cela, nous explorons dans ce mémoire un mécanisme peu utilisé jusqu'à maintenant, l'identité numérique, afin de voir son potentiel dans la construction d'une 'confiance assurée' entre pairs des échanges collaboratifs. Pour ce faire, nous posons d'abord les bases en rappelant ce qu'est l'économie collaborative. Nous enchaînons avec une revue des principaux mécanismes de construction de la confiance utilisés par les plateformes de cette économie afin de déceler leurs avantages, inconvénients et manquements. Ensuite, nous approfondissons le principe d'identité numérique afin de mieux le cerner dans ses fonctionnalités et ses enjeux. Enfin, nous analysons trois projets européens de développement d'une architecture d'identité numérique. Au cours de nos recherches, nous nous sommes rendus compte de l'ampleur du travail nécessaire à la bonne compréhension de ceux-ci, étant donné leur complexité. Ainsi, chacun d'entre eux mériterait un mémoire dédié mais nous avons voulu effectuer une première exploration de ces trois projets afin d'en détecter les potentiels respectifs dans leur capacité à restaurer une confiance assurée dans l'économie collaborative. Pour les analyser, en saisir leurs potentiels et leurs spécificités, nous nous basons sur une grille d'analyse portant sur dix critères. Cette analyse nous permet de dégager les points forts mais aussi les limites respectives de ces trois projets en matière d'établissement d'une "confiance assurée" lors de transactions collaboratives.

Mots Clés
Identité numérique, économie collaborative, construction de la confiance, mécanisme de confiance,

Table des matières

1 Introduction

1.1 Mise en contexte

De nos jours, il est rare de trouver quelqu'un n'ayant jamais rien acheté en ligne. Que ce soit sur l'e-shop d'une enseigne bien connue, sur des pages de petits marchands, sur des plateformes collaboratives ou encore sur les réseaux sociaux, nous achetons, commandons, échangeons de plus en plus de biens et de services via internet. Ces transactions s'effectuent ainsi par le biais de plateformes dédiées, mettant en relation vendeurs et acheteurs. Certains sites d'e-commerce sont directement vendeurs de bien et/ou services (on parle alors de « B2C », pour « Business To Customer ») tandis que d'autres plateformes s'occupent, elles, de mettre en relation des particuliers (on parle alors de « P2P », pour « Peer to Peer »). De la vente de vêtement au service de bricolage, du covoiturage à la location de chambres, de l'échange de maison au prêt de voiture, les plateformes collaboratives se sont multipliées ces dernières années et tout ou presque est dorénavant trouvable et disponible sur ces sites.

Ainsi, en marge du commerce dit « traditionnel », il y a ces plateformes qui favorisent les interactions entre particuliers pour l'échange ou l'achat de biens et services. C'est sur ces plateformes que nous allons nous pencher tout au long de ce mémoire, et plus particulièrement sur les mécanismes liés à la construction et au maintien de la confiance entre les partenaires de la transaction.

1.2 Économie collaborative

Une des branches du commerce en ligne est l'économie collaborative, mentionnée dans le point précédent sous l'acronyme « P2P ». Uber, Airbnb, Vinted, BlaBlaCar, eBay, pour ne citer qu'elles, tous ces noms nous sont aujourd'hui familiers et semblent bien ancrés dans nos quotidiens. Ce genre de plateforme prend de plus en plus d'importance et attire l'attention des chercheurs, comme le disent (Teubner et Dann 2018, p.1)[31] : « Two-sided platform business models have gained accelerating importance and research attention over the last years ». Cependant, comme le souligne (Belleflamme 2017, p.1)[11] : « L'économie dite "collaborative" ou "du partage" demeure un concept assez flou, sans définition claire et largement acceptée ».

Toutefois, précise l'auteur, il n'est pas compliqué de comprendre les bases de leur mode de fonctionnement. Ces plateformes dites "collaboratives" ou "partagées" ne sont pas gérées comme telles. « Elles s'inscrivent complètement dans l'économie de marché traditionnelle » (Belleflamme 2017, p.1)[11], mais favorisent néanmoins une certaine forme de partage entre leurs utilisateurs. « (...) elles facilitent l'échange de biens et services entre "pairs" » où « le terme "pair" est employé pour souligner que dans la plupart des cas, les utilisateurs de ces plateformes peuvent y opérer indifféremment du côté de l'offre ou du côté de la

demande. Il n'y a donc pas, a priori, d'identification claire des rôles de chacun » (Belleflamme 2017, pp.1-2)[11]. Comme le disent également si bien (Philippette, Collard et Klein 2016, p.1)[28] : « L'économie collaborative d'aujourd'hui repose sur une logique contributive où l'homo oeconomicus n'est plus un simple consommateur mais devient aussi un producteur, commentateur ou facilitateur ».

Il existe toutefois une différence fondamentale et cruciale entre une plateforme d'e-commerce traditionnelle et une plateforme de pair à pair. Lorsqu'on achète un produit sur le site d'un marchand reconnu, on ne se pose en général pas trop de questions.
En effet on ne se demande pas :

— Ma commande va-t-elle vraiment arriver à destination ?
— Le produit correspond-t-il à la description ?
— La personne en charge de réaliser le service est-elle vraiment qualifiée ?
— ...

ou en tout cas dans une moindre mesure, même s'il existe bien entendu des sites qui font exception et pour lesquels les utilisateurs feront toujours preuve de méfiance. Ceci s'explique par le fait que, bien souvent, les sites d'e-commerce ne sont que les boutiques en ligne de magasins qui existent physiquement ou d'enseignes connues. Par conséquent, pour bon nombre de sites, acheter en ligne revient à acheter un bien dans son magasin préféré mais depuis la maison. Lorsqu'un marchand fonctionne cent pourcent en ligne, le raisonnement est sensiblement le même dans le sens où un utilisateur se persuadera qu'il est peu probable qu'une entreprise, car c'est une entreprise qui se "cache" derrière le site, pas un particulier, tente de l'escroquer ouvertement. En effet, ce type de comportement aurait un effet quasi immédiat sur sa réputation et sa survie économique. Le problème ne se poserait alors que pour les marchands très peu connus, comme le souligne (Farhani 2014, p.2)[19] : « Ce problème se pose particulièrement pour le cyber marchand peu connu ou inconnu, car l'image de marque contribue dans une large mesure à établir un niveau de confiance susceptible de rassurer les internautes ». Tandis qu'une plateforme classique et connue entretient avec l'utilisateur un sentiment de confiance presque évident et naturel (confiance dite institutionnelle, nous y reviendrons plus tard), sur une plateforme collaborative ce sont principalement les utilisateurs qui, entre eux, doivent établir un niveau de confiance suffisant pour que les échanges, achats (...) de biens et services puissent se faire. Les plateformes dites collaboratives participent à cette construction de la confiance entre particuliers de manière indirecte en proposant divers mécanismes censés les aider à développer cette confiance mutuelle. Mais, ce sont bien les utilisateurs qui, à l'aide de ces mécanismes, se forgent leur propre opinion des pairs avec qui ils doivent interagir et ainsi déterminent s'ils peuvent ou non se faire confiance. Du résultat de cette évaluation bilatérale dépendra l'issue d'une transaction. Car selon (Teubner et Dann 2018, p.1)[31] : « Typical users of C2C platforms are non-professional individuals with neither an established brand image nor global recognition. In addition, many C2C transactions yield high economic, social, and physical exposure ». Ceci implique que les utilisateurs de ces plateformes de l'économie collaborative doivent pouvoir

se faire suffisamment confiance pour accepter de s'exposer à ces risques, comme le soulignent (ter Huurne, Ronteltap, Corten et Buskens 2017, p.1)[30] : « Users and potential users of the sharing economy need to place a considerable amount of trust in both the person and the platform with which they are dealing. The consequences of transaction partners' opportunism may be severe, for example damage to goods or endangered personal safety ».

1.3 Question de recherche et déroulé du mémoire

Nous venons de l'aborder, la confiance est donc un élément central dans l'utilisation des plateformes de la "sharing economy", comme l'affirment (ter Huurne, Ronteltap, Corten et Buskens 2017, p.1)[30] : « Trust is, therefore, a key factor in overcoming uncertainty and mitigating risk ». Aussi, selon (Teubner et Dann 2018, p.1)[31] : « As such business models rely on the realization of transactions among peers, a central aspect to virtually all platforms are the creation and maintenance of peer-trust ». Tous ces auteurs mettent en avant l'importance du rôle de la confiance pour l'utilisation de ces plateformes collaboratives puisque, selon eux, elles doivent toutes travailler autour de cet aspect central qu'est la création et le maintien de la confiance entre les pairs pour surmonter l'incertitude et diminuer les risques. En effet, selon (Ert, Fleischer et Magen 2016)[18] pour qu'une transaction puisse aboutir : « (...) two strangers are unlikely to engage in a monetary transaction without trusting one another ».

Nous pouvons ainsi dire qu'il existe un consensus quant à la nécessité de favoriser, d'une manière ou d'une autre, la construction de la confiance entre les différents acteurs d'une transaction. Il n'existe pourtant pas de résultats de recherche solides et validés concernant la manière dont la confiance se développe dans l'économie collaborative, selon (ter Huurne, Ronteltap, Corten et Buskens 2017, p.1)[30] : « (...) there is no thorough overview of how trust is developed in this context ».

Par conséquent, il nous est paru primordial d'explorer et de questionner les mécanismes mis en place par les plateformes pour favoriser l'établissement d'un niveau de confiance suffisant entre les utilisateurs afin que des transactions aient lieu. Nous nous posons ainsi cette question : « Quels sont les mécanismes mis en place par les plateformes de l'économie collaborative permettant d'aider les utilisateurs à développer un certain niveau de confiance mutuelle, les amenant par la suite à conclure une vente ou un échange de bien ou de service, mais surtout, à accepter de s'exposer au risque monétaire, matériel et/ou physique que comporte une transaction avec un(e) inconnu(e) ? ».

Afin de répondre à cette question, nous allons d'abord faire le point sur la confiance en explorant ce concept qui s'avère finalement assez abstrait. Nous poursuivrons ensuite avec une présentation et une évaluation des principaux mécanismes de construction de la confiance actuellement utilisés par les plateformes de l'économie collaborative. Nous consacrerons la suite du mémoire à l'exploration d'un mécanisme de confiance peu étudié jusqu'ici, à savoir l'identité numérique. Pour ce faire, nous élaborerons une grille d'analyse qui nous permet-

tra par la suite d'analyser et évaluer trois projets européens de développement d'une identité numérique. Nous les comparerons et nous expliquerons, sur bases des critères de la grille, en quoi ils peuvent ou non apporter une réponse à notre problématique de la confiance et dès lors être bénéfiques à l'économie collaborative. Nous finirons par une conclusion qui nous permettra d'émettre des pistes d'amélioration pour le futur de l'économie collaborative et qui synthétisera les propos de ce mémoire.

2 Économie collaborative et confiance : Revue des principaux mécanismes

2.1 Introduction

Ce chapitre a pour objectif de placer un cadre théorique autour de la confiance car, comme nous l'avons vu précédemment, c'est un élément central pour le modèle économique de l'économie collaborative. Le chapitre a aussi pour but d'effectuer une revue des mécanismes favorisant la construction de la confiance sur les plateformes de l'économie collaborative.

Pour ce faire, nous allons d'abord parcourir le concept de la confiance afin de mieux le cerner. Il est primordial de pouvoir la définir correctement pour être en mesure d'identifier les mécanismes et d'expliquer en quoi ils aident les utilisateurs à forger leur confiance. Ensuite, nous parcourrons les mécanismes les uns après les autres afin d'en extraire les avantages ainsi que, le cas échéant, les limitations.

2.2 Le concept de confiance

Nous pourrions donner une définition simple et concise en citant (Lobet 2018, p.3)[24] : « (...) on peut dire que la confiance est ce qui permet de suspendre le doute pour s'engager dans une action ou une relation. Elle est ce qui permet le "saut" dans l'engagement en situation d'incertitude ». Ce qui rejoint des auteurs que nous avons vu précédemment (Ert, Fleischer et Magen 2016)[18], selon lesquels il est peu probable que des utilisateurs de plateformes collaboratives s'engagent dans une transaction s'ils ne se font pas confiance.

Néanmoins, selon (Luhmann 2001)[25], il convient de faire la distinction entre deux types de confiance. Cet auteur différencie en effet ce qu'il appelle la confiance assurée (*confidence*) de la confiance décidée (*trust*). Ainsi, ces deux types de confiance, bien que parfois complémentaires, ne se manifestent ni de la même manière ni dans les mêmes situations. « Les deux concepts font référence à des attentes qui peuvent être déçues. (...) Vous êtes assurés que vos attentes ne seront pas déçues (*confident*) : que les hommes politiques essaieront d'éviter la guerre, que les voitures ne tomberont pas en panne, ou qu'elles ne quitteront pas soudainement la route pour venir vous renverser (...) » (Luhmann 2001, p.8)[25]. Selon cet auteur, c'est le type de confiance pour lequel nous n'avons rien à faire, et qui nous permet de vivre sans être indéfiniment sur le qui-vive.

Ainsi, nous devons « (...) plus ou moins ne pas tenir compte de la possibilité que nos attentes soient déçues. (...) L'alternative est de vivre dans un état d'incertitude permanente et de renoncer à vos attentes sans avoir rien d'autre à mettre à leur place » (Luhmann 2001, p.8)[25]. C'est cette confiance assurée qui nous permet ainsi de lever nos doutes parce que nous savons que nous pouvons prendre certains "risques", et que, normalement, tout se passera bien. Nous nous en remettons dans ce cas à ce que l'auteur appelle des "attributions externes". Ce sont les organismes de contrôle sur lesquels nous basons notre confiance assurée. Ainsi, nous partons tous les jours travailler sans être armés car nous avons confiance en la police et son travail. Tous les jours nous prenons notre voiture sans pour autant nous équiper de l'attirail du garagiste car nous plaçons notre confiance dans les concepteurs de nos véhicules. Si maintenant il s'avère que nous nous trompons, nous nous en remettrons dans ce cas à ces autorités, à ces attributions externes en nous demandant s'ils ont assuré correctement leur responsabilité. C'est une manière de se décharger de la responsabilité d'avoir fait confiance aveuglément. En ce qui concerne la confiance décidée, il faut avoir à l'esprit qu'« elle requiert un engagement préalable de votre part. Elle présuppose une situation de risque. Vous pouvez acheter ou ne pas acheter une voiture d'occasion qui s'avérera être une "épave". Vous pouvez engager ou ne pas engager une baby-sitter pour la soirée et lui confier votre appartement sans surveillance ; elle pourra être aussi être une "catastrophe". Vous pouvez éviter de prendre le risque, mais seulement si vous acceptez de renoncer aux avantages associés » (Luhmann 2001, p.8)[25]. Il faut avoir en tête que l'évaluation du risque est une affaire totalement subjective, personnelle : « (...) la perception et l'évaluation du risque sont une affaire hautement subjective. Elles différencient les gens et promeuvent des types différents d'individualité : l'un recherche les risques, l'autre les évite ; l'un fait confiance, l'autre se méfie » (Luhmann 2001, p.13)[25]. Pour citer (Lobet 2018, p.5) : « (...) cette confiance n'est ni automatique, ni collective ou partagée. Elle repose sur un choix personnel, une décision qui demande calcul et raison ». « C'est un calcul purement *interne* de conditions *externes* qui crée le risque » (Luhmann 2001, p.12)[25].

Il est clair maintenant que les confiances assurée et décidée ne "s'appliquent" pas aux mêmes "systèmes". Cependant, selon (Luhmann 2001, p.16)[25], des liens peuvent exister entre elles : « Les grands systèmes fonctionnels dépendent non seulement de la confiance assurée, mais aussi de la confiance décidée. Si la première manque, il y aura un sentiment diffus de non-satisfaction, de désaffection ou même d'anomie ; il se peut que cela n'ait aucun impact immédiat sur le système. Si la seconde fait défaut, par contre, cela change la façon dont les gens prennent leurs décisions sur les questions importantes ». En effet, encore selon (Luhmann 2001, p.17)[25] : « Quant au défaut de confiance décidée, il conduit simplement à s'abstenir d'agir. Il réduit la gamme des possibilités d'actions rationnelles. (...) Le manque de confiance décidée peut provoquer le rétrécissement d'un système ; celui-ci peut même tomber, du point de vue de sa taille, sous le seuil critique nécessaire à sa propre reproduction à un certain niveau de développement ».

Sur base de cette conception de la confiance, il nous semble important de

souligner que si la participation à une transaction entre pairs relève bien de la confiance décidée, celle-ci peut être allégée ou 'rassurée' par la mise en place de 'mécanismes de confiance' sur ces plateformes collaboratives. Nous allons dès lors consacrer la section suivante à la présentation et l'analyse de ces mécanismes dans ce qu'ils permettent ou pas en terme d'établissement de la confiance entre pairs.

2.3 La confiance dans l'économie collaborative - État de l'art sur les mécanismes de construction de la confiance

Dans cette section, nous allons faire l'état de l'art concernant les mécanismes de construction de la confiance dans l'économie collaborative. Ces mécanismes sont censés soulager la 'confiance calculée' nécessaire à l'engagement de pairs dans une transaction collaborative. Il est donc important d'identifier ces mécanisme, de les analyser afin d'évaluer leur valeur pour la construction de la confiance.

2.3.1 Mécanismes

En 2018, (Teubner et Dann 2018)[31] ont mené une étude dans laquelle ils analysent onze plateformes de différents domaines, toutes issues de l'économie collaborative. Sur base de cette étude, ils ont classé les mécanismes de construction de la confiance en quatre catégories :

- **Catégorie 1 : Mécanismes basés sur les transactions**
  - **Notation :** Sous forme de points ou d'étoiles, c'est le score que l'on donne à l'autre pair une fois la transaction effectuée ou le service rendu.
  - **Commentaire :** Cette fois-ci sous forme de texte, c'est l'évaluation que l'on fait de l'autre pair une fois la transaction effectuée ou le service rendu.
- **Catégorie 2 : Profils d'utilisateurs**
  - **Photo de profil :** Fonctionnalité assez classique, qui permet à un utilisateur d'uploader une photo sur son profil en ligne.
  - **Auto-description :** C'est en général ce qui permet aux utilisateurs de se présenter, afficher leurs centres d'intérêts, leur âge, d'où ils viennent,...
- **Catégorie 3 : Vérification d'identité**
  - **Email :** Ce mécanisme consiste en l'envoi d'un email à la personne qui s'inscrit, qui doit alors être validé par cette dernière, au moyen d'un lien cliquable par exemple.
  - **Téléphone :** Ce mécanisme consiste en l'envoi d'un SMS au numéro renseigné, souvent contenant un code qui doit alors être introduit par l'utilisateur pour confirmation d'inscription sur la plateforme.
  - **ID :** Vérification d'identité plus poussée. Par exemple, en Belgique, il est possible de se connecter à certains sites prioritaires au moyen

de la carte d'identité officielle.
    - **Réseaux sociaux :** Mécanisme par lequel il est possible d'utiliser le compte d'un réseau social (comme Facebook, Google,...) pour se connecter.
- **Catégorie 4 : Informations implicites**
  Il s'agit ici de statistiques donnant un aperçu rapide de l'implication d'un utilisateur sur une plateforme. Les auteurs prennent en compte :
    - **Nombre de transactions :** Le nombre de transactions, permet de voir assez facilement l'implication d'un utilisateur sur la plateforme, s'il a conclu beaucoup d'affaires ou pas.
    - **Nombre de commentaires :** Le nombre de commentaires, comme le nombre de transactions, peut être un bon indicateur de l'implication d'un utilisateur sur la plateforme.
    - **Inscrit depuis :** Cet indicateur permet aux autres utilisateurs de voir rapidement depuis quand un utilisateur est inscrit sur une plateforme.

Nous aurions pu croire que la construction de la confiance se fait uniquement sur base de la réputation accumulée des utilisateurs mais il n'en est rien, comme nous avons pu le voir avec les catégories ci-dessus de (Teubner et Dann 2018)[31] et comme le disent également (ter Huurne, Ronteltap, Corten et Buskens 2017, p.1)[30] : « Trust in this economy is often reduced to the use of reputation systems alone. However, our study suggests that trust is much more complex than that and extends beyond reputation ». (Teubner et Dann 2018, p.3)[31] affirment d'ailleurs encore autrement que la confiance ne se réduit pas à un système de réputation, mais bien à un ensemble de techniques puisque tous les mécanismes identifiés sont retrouvés dans toutes (ou presque) les plateformes présentes dans leur étude : « As can be seen there, many of the identified artefacts such as rating scores, text reviews, and profile images are present on basically every platform, while others are less common (e.g., social media linkage). (...) Most of the studied platforms employ all four basic types of trust-building mechanisms (transaction-based assessments, expressive user profiles, identity verification, display of implicit information ». Cependant, il faut noter que les utilisateurs ne font pas usage des mécanismes de la même manière en fonction des plateformes, comme le soulignent (Teubner et Dann 2018, p.4)[31] : « Despite several similarities, there exist marked crossplatform differences in how these mechanisms are being utilized by the platforms' users ».

2.3.2 Réputation

La réputation fait partie de la première catégorie de (Teubner et Dann 2018)[31]. Ces systèmes sont apparus avec le développement des premières plateformes d'échange de pair à pair (Hadhri, Lemoine et Guesmi 2017, p.8)[20]. À la fin de chaque transaction, l'utilisateur "receveur" est amené à donner une note ou un commentaire (parfois les deux) à l'utilisateur "donneur". Cela afin d'apprécier ou non ses qualités en tant que vendeur/prestataire/loueur/... Parfois, il est également possible pour ce dernier de donner une évaluation à celui qui

bénéficie du service, de la location d'un bien ou qui tout simplement achète un bien. Cela se fait notamment sur eBay, où le vendeur peut ainsi évaluer l'acheteur, en mettant par exemple en avant ses qualités de bon payeur, la rapidité avec lequel le paiement a été effectué, la courtoisie,... « Ces systèmes de réputation font alors office d'un véritable bouche à oreilles électronique » (Hadhri, Lemoine et Guesmi 2017, p.8)[20].

Le mécanisme de réputation semble prometteur mais que pouvons-nous dire sur l'efficacité de ce mécanisme ? Les utilisateurs font-ils vraiment attention aux résultats de ce système ? Les plateformes fournissent-elles toutes le même système de réputation ?

Nous pouvons déjà répondre "non" à la dernière de ces questions. En effet, (Teubner et Dann 2018, p.3)[31] ont, au travers de leur étude, montré que les plateformes n'implémentent pas les mécanismes de la même manière : « (...) there occur considerable and platform-contingent differences in how these tools and mechanisms are actually being used ». Ainsi, ce mécanisme varie en termes d'échelle, de calcul, de granularité et d'affichage en fonction des plateformes. En effet, alors que certaines vont proposer un affichage en étoiles, d'autres vont proposer un affichage avec une note sur dix. D'autres proposeront alors une note sur cinq. D'autres encore utiliseront une note sur dix mais avec une granularité tous les 0,1 plutôt que des 0,5... Cependant, les plateformes présentent des schémas similaires en terme d'asymétrie du score (Teubner et Dann 2018, p.3)[31] : « (...) most platforms exhibit rather similar patterns of rating score skewness, while there exist outliers in both directions ». Cela veut dire que malgré les différences qu'il peut y avoir dans la granularité des scores d'une plateforme à l'autre, les notes octroyées entre utilisateurs, elles, semblent se répartir de la même manière.

Nous pouvons ensuite affirmer que, bien que les utilisateurs ne participent pas aux plateformes collaboratives pour leur système de réputation (Sung-Byung, Kyungmin, Hanna et Chulmo 2019, p.2)[34] : « (...) examined what drives people to participate in sharing economy, and they concluded that user enjoyment and economic benefits are important motivations, while consumption sustainability and reputation are either a partially or not influential factor to users' motivation », ils font cependant attention aux systèmes de réputation pour construire leur confiance : « (...) highlighted that trust and reputation are influential factors within a provider-receiver relationship » (Sung-Byung, Kyungmin, Hanna et Chulmo 2019, p.2)[34]. Une étude de (Abrahao, Parigi, Gupta and Cook 2017)[10] a démontré que les systèmes de réputation permettent de palier à certaines tendances qu'ont les Hommes à baser leur confiance sur des préjugés sociaux, et plus particulièrement celle qui consiste à faire confiance en des personnes qui nous sont similaires. Ils se sont notamment concentrés à déterminer dans quelle mesure les systèmes de réputation peuvent atténuer voire dépasser cette tendance qu'est l'homophilie. Les auteurs de l'étude ont fait participer 8906 utilisateurs de la plateforme Airbnb (dont 6714 participations étaient exploitables car complètes - étude rémunérée afin d'éviter et limiter les biais, ainsi qu'encourager les bons comportements), à un jeu d'investissement interpersonnel. Les participants commencent l'expérience avec un certain montant,

et doivent investir des parties de ce montant en d'autres candidats dont les profils sont proposés à l'écran. Les chercheurs font alors varier les caractéristiques de ces profils afin d'étudier l'interaction entre l'homophilie et la confiance. Leur étude a montré que, bien qu'une tendance à l'homophilie a pu être observée et confirmée, un système de réputation peut influencer cette tendance initiale. Ainsi, les participants de l'étude ont montré qu'ils sont enclins à étendre leur réseau de confiance envers des personnes présentant moins de caractéristiques communes avec eux si leur niveau de réputation est élevé : « Our findings show that reputation systems can significantly increase the trust between dissimilar users and that risk aversion has an inverse relationship with trust given high reputation » (Abrahao, Parigi, Gupta and Cook 2017, p.1)[10]. D'autres auteurs (Sung-Byung, Kyungmin, Hanna et Chulmo 2019, p.3)[34] les rejoignent en ce sens : « Another unique quality of the sharing economy concerns the personal nature (e.g., values, lifestyles, likes or dislikes, preferences, and commomnalities) of individuals. (...) when sharing and recipient parties recognize similarities, it could diminish their concerns about transaction risks ».

Malgré cela, il subsiste d'autres biais pour les systèmes de réputation (Hadhri, Lemoine et Guesmi 2017, p.8)[20]. Notamment celui de "non réponse", qui survient lorsque les utilisateurs ne laissent aucune note ou aucun commentaire une fois une transaction terminée. Ce taux de non réponse est rarement comptabilisé dans les statistiques de réputation, ce qui peut biaiser la fiabilité de l'indice. Un autre biais est celui des "représailles". Néanmoins, ces biais peuvent "facilement" être évités, par exemple en ne révélant les notes que lorsque les deux parties se sont exprimées (Zervas, Prosperio et Byers 2015, p.5)[35] : « (...) to limit strategic considerations in providing feedback (e.g., to limit retaliatory reviewing), Airbnb changed its reputation system to simultaneously reveal reviews only once both parties supply a review for each other, or until 14 days had elapsed from the conclusion of the trip, whichever occurred first. After 14 days, no further reviewing of a completed trip is allowed ». Cela n'est par contre par le cas sur chaque plateforme, et cette peur des représailles influence directement l'efficacité de ce système puisque les protagonistes s'arrangeront alors pour se noter de manière positive mutuellement. Selon (Slee 2013, pp.6-7) : « Collusion and fear of retaliation are the reasons why there are essentially no reviews less than five stars for rides that take place. If you give a less-than-five star review then, unlike in the case of offline community-based testimonials, it is visible to the reviewee, who can give you a harsh review in return and so affect your chance of getting future rides. (...) but so long as you give me five stars I'll give you a good positive rating and we're both better off ». Pour terminer avec les propos de (Slee 2013, p.7) : « So even in the absence of explicit gaming, peer-to-peer internet reputation systems do not solve the problem of trust ».

2.3.3 Profils

« Faces create trust » (Teubner et Dann 2018, p.3)[31]. Il n'est donc pas surprenant, selon les auteurs, que presque toutes les plateformes donnent la possibilité aux utilisateurs d'uploader une photo de profil. Dans le comparatif effectué par ces deux auteurs, il n'y a qu'une plateforme sur les onze, qui ne permet pas la mise en ligne d'une photo de profil. Bien que l'on pourrait croire qu'une photo de profil n'apporte pas grand chose, il n'en est rien. Il a même été montré qu'en fonction des plateformes, elles ne sont pas utilisées de la même manière par les utilisateurs finaux. Alors qu'il est par exemple possible de mettre une photo de profil sur eBay et Airbnb, les données montrent que la quasi totalité des utilisateurs d'Airbnb (99,8%) en ont mise en ligne, contre seulement 15,8% des utilisateurs d'eBay (Teubner et Dann 2018)[31]. De plus, une étude relatée par ces auteurs, effectuée par Microsoft, indique qu'une analyse par reconnaissance faciale des utilisateurs a pu détecter des visages reconnaissables sur leur photo, de l'ordre de 1% des profils d'eBay contre 92% des profils de TaskRabbit. Ce qui démontre bien que d'une plateforme à l'autre, les utilisateurs ne font pas le même usage d'un même mécanisme.

Selon (Ert, Fleischer et Magen 2016)[18], cette confiance basée sur le visuel affecte le comportement du consommateur au moins autant que, si pas plus que, la réputation du vendeur telle que communiquée par son score. Toujours selon eux (Ert, Fleischer et Magen 2016, p.2)[18], une étude récente sur les logements proposés par Airbnb à New York City apporte des preuves selon lesquelles les photos de profil faciliteraient la discrimination raciale : « A recent study on Airbnb listings in New York City provides supporting evidence for our assertion by suggesting that personal photos might facilitate racial discrimination ». Il y a donc des raisons de penser que l'effet potentiel des photos de profils en ligne va bien au-delà de leur simple présence, et qu'elles ont un réel impact sur le processus de construction de la confiance (Ert, Fleischer et Magen 2016, p.3)[18] : « (...) there are reasons to believe that the potential effect of photos on online consumers goes beyond their mere presence ». Ils suggèrent que lorsqu'un individu voit la photo de profil d'une autre personne, il émet un jugement instantané sur ses attributs sociaux. Ils relaient notamment une étude de neuroscientifiques selon lesquels ce mécanisme serait intuitif et automatique. Notre cerveau serait également capable de se former un jugement de la confiance que dégage une personne, sur base d'une photo, en moins d'une seconde. Ils relaient également un phénomène qui a été nommé la « beauty premium ». Cela suggère que des utilisateurs d'apparence plus attrayants étaient perçus comme étant plus dignes de confiance (Ert, Fleischer et Magen 2016, p.9)[18] : « (...) some evidence of a "beauty premium" ; attractive hosts are more likely to be chosen over less attractive ones ».

Quoiqu'il en soit, des études récentes sur la confiance dans les plateformes collaboratives ont montré que les informations fournies par les utilisateurs sur leur profil et les photos de profil influencent les processus de construction de la confiance et de prise de décision (Sung-Byung, Kyungmin, Hanna et Chulmo 2019)[34]. Néanmoins, il est important de rappeler que les photos de profil

peuvent être fausses ou trafiquées car rien n'empêche un utilisateur de publier ce que bon lui semble. Par conséquent, il est étonnant de voir que les photos de profil puissent ainsi autant stimuler la construction de la confiance.

2.3.4 Identité Digitale

Les mécanismes de vérification d'identité ne sont pas aussi répandus parmi les plateformes que le sont, par exemple, les photos de profil et les scores (Teubner et Dann 2018, p.4)[31] : « Mechanisms for identity verification are not as widely used across platforms as, for instance, profile images and rating scores ». Même parmi les plateformes qui les proposent, ce n'est pas toujours obligatoire. Par exemple, il est possible de prendre une photo de la carte d'identité sur Airbnb mais cela n'est pas bloquant si cela n'est pas fait. Certaines plateformes ne font, elles, parfois même l'usage d'aucun de ces systèmes de vérification d'identité, toujours selon (Teubner et Dann 2018)[31].

D'autres plateformes, comme TaskRabbit par exemple, jouent par contre un rôle spécial en ce qui concerne la vérification d'identité, puisque selon la plateforme elle-même, tous les travailleurs subissent un processus approfondi de vérifications et d'accompagnement personnel. Même si cela n'est pas explicitement indiqué sur leur profil, nous pouvons supposer que tous les travailleurs de la plateforme ont été dûment vérifiés (Teubner et Dann 2018)[31]. Nous connaissons une autre plateforme qui effectue le même genre de vérification, à savoir "ListMinut", qui affiche clairement sur son site internet : « Nous rencontrons personnellement et sélectionnons nos prestataires au préalable ».

2.3.5 Mécanismes Indirects

Au-delà des mécanismes conçus pour accroître la confiance, les plateformes utilisent également des moyens pour diminuer les risques et ainsi réduire le seuil de confiance nécessaire à l'accomplissement d'une transaction (Teubner et Dann 2018)[31]. Cela inclut des "mécanismes" tels que des assurances, des garanties,... Toujours selon (Teubner et Dann 2018, p.2)[31], en plus de la confiance entre les partenaires d'une transaction, la confiance dans la plateforme elle-même représente une condition préalable à la concrétisation des transactions : « In addition to trust into prospective transaction partners, also trust into the platform itself represents a prerequisite for transactions to materialize. Importantly, a platform's trustworthiness is suggested to rub off on the providers on the platform ». D'autres auteurs comme (Hadhri, Lemoine et Guesmi 2017, p.7)[20] évoquent un « (...) transfert de la confiance de la plateforme vers les tiers ». En effet, ils estiment que le volume d'échange, l'ancienneté et la réputation de la plateforme peuvent par exemple faire naître un sentiment de sécurité chez l'utilisateur. L'idéal est, bien entendu, que l'utilisateur ait une confiance presque "aveugle" ou, pour reprendre les mots de (Luhmann 2001)[25], une confiance « assurée », presque automatique envers la plateforme. Cela afin que l'utilisateur n'ait plus qu'à se soucier de « décider » s'il peut faire confiance à un autre utilisateur ou non.

(Teubner et Dann 2018, p.4)[31] font également allusion à la possibilité de discuter avec l'autre utilisateur faisant partie de la transaction, avant de conclure. Ceci permettrait d'écarter certains préjugés, qui auraient pu être faits sur la simple base d'un profil pas assez détaillé, ou d'un manque de réputation,... Bien que dans certains cas cela permette de lever les doutes quant à l'autre utilisateur de manière positive, il est difficilement vérifiable sur base de la littérature consultée que le simple fait de discuter brièvement, de surcroît sans visu, avec une autre personne permette purement et simplement de lever les doutes et les incertitudes générés par l'interaction avec un inconnu.

2.4 Conclusion et Discussion

Dans cette conclusion, nous souhaiterions mettre en discussion les enseignements tirés de l'examen de ces mécanismes sur base d'un exemple personnel de transaction. Ceci nous permettra d'éclairer le choix que nous avons fait de travailler sur l'identité numérique comme un dispositif ouvrant à de nouvelles perspectives en matière de confiance dans les échanges collaboratifs.

Lors de la vente d'un bien personnel (dont la valeur avoisinait les 1100€) sur l'une de ces plateformes, nous avons été confronté à ce problème de confiance et c'est alors que des questions la concernant ont commencé à émerger. Cela peut paraître anodin mais cette expérience a été la source de beaucoup de stress et d'angoisses. Allons-nous être payé ? L'argent en liquide (si paiement en liquide) sera-t-il réel ? Les acheteurs vont-ils nous agresser et partir avec le bien sans payer lors de l'échange ? Allons-nous envoyer un colis et ne jamais recevoir le montant attendu en échange ? Tant de questions qui peuvent paraître pessimistes ou peureuses mais qui se posent pourtant lorsque nous ne savons pas à qui nous avons affaire. Et même lorsque nous acceptons le risque de nous lancer dans l'inconnu, d'autres questions peuvent alors surgir. Quel(s) recours aurons-nous en cas de litige, de fraude ou d'arnaque ? Pourrons-nous être remboursés ?

Il nous est alors venu à l'esprit que la seule manière d'être à cent pour cent certains de ne pas avoir de problème serait d'avoir affaire à des utilisateurs dont les profils auraient été vérifiés de manière officielle. Nous entendons par "officielle" une vérification permettant de lier chaque utilisateur enregistré sur une plateforme à une personne réelle. Cette idée nous a paru aussi évidente du fait que, a priori, nul n'aurait envie d'être l'auteur d'arnaques ou de fraudes s'il est si facilement identifiable. Les plateformes pourraient alors également s'échanger des informations de réputation sur base d'un profil commun, comme le suggèrent (Teubner et Dann 2018, p.4)[31] : « In view of the multiplicity of platforms and the many parallel, unconnected reputation silos, recent research has set out to consider the transfer of reputation between platforms ». Nous savons qu'il existe de tels services d'identité numérique, en Belgique par exemple (itsme ®), mais ce n'est pas le cas dans tous les paysPar ailleurs, l'utilisation de ce genre de système sur les plateformes collaboratives n'est pas encore très répandue, comme vu plus haut (Teubner et Dann 2018, p.4)[31] : « Mechanisms for identity verification are not as widely used across platforms as, for instance, profile images and rating scores ». De plus, les coûts de ce genre de service

sont très importants. En effet, nous avions fait la demande de devis à ce service d'identité numérique dans le cadre d'un projet de création d'une plateforme de seconde main mettant à disposition des utilisateurs un système d'authentification forte afin de limiter les fraudes. Suite à la découverte des coûts liés à ce système d'identité numérique, notre projet s'est arrêté à l'étude. Nous savons également qu'il est possible de permettre à un utilisateur de se connecter via des comptes de réseaux sociaux tels que Facebook ou un compte Google, pour ne citer qu'eux, mais selon nous cela n'est pas gage de sécurité étant donnée la facilité déconcertante avec laquelle il est possible de créer un faux compte sur ces réseaux sociaux actuellement.

Dans ce mémoire, nous souhaitons explorer l'identité numérique afin de comprendre son fonctionnement mais aussi d'analyser son potentiel en matière de création de la confiance entre partenaires de l'économie collaborative. Cette orientation de notre travail repose tout d'abord sur notre expérience personnelle, telle que nous venons de la décrire. En effet, la revue de la littérature que nous avons réalisée pour consolider cette hypothèse montre que les recherches qui lient confiance, identité numérique et économie collaborative sont très peu nombreuses, voire inexistantes. Ceci semble attesté par (Ert, Fleischer et Magen 2016, p.2)[18] quand ils soulignent : « (...) most of the literature concerning trust in e-commerce addresses the role of online reviews ». Mais cette orientation s'inscrit aussi en conclusion de la revue à laquelle nous venons de procéder concernant les mécanismes de confiance existants sur les plateformes collaboratives. Mis à part la vérification 'humaine' de l'identité des personnes, telle que la pratique par exemple 'ListMinute' mais qui se révèle très coûteuse en ressources, chacun des autres mécanismes possède, comme nous l'avons montré, des failles et des biais. Dès lors, les usagers des plateformes collaboratives semblent réduits aujourd'hui à devoir développer une sorte de "flair digital" combinant différentes informations à leur disposition afin de prendre une décision quant à l'octroi de leur confiance, ou quant à la prise de risque (au choix) envers un autre utilisateur. Nous sommes dès lors bien dans ce que (Luhmann 2001)[25] appelle une confiance calculée : « (...) calcul rationnel (...) » (p.8) ou encore un « (...) calcul purement interne de conditions externes (...) » (p.12). C'est ce poids du calcul, cette difficulté à s'engager dans l'incertain que l'identité numérique pourrait aider à réduire. C'est du moins l'hypothèse que nous formulons.

3 Identité numérique

3.1 Introduction

Puisque nous émettons l'hypothèse selon laquelle l'identité numérique serait une solution pour régler les problèmes actuels de construction de la confiance sur les plateformes de l'économie collaborative, il est maintenant important de définir ce concept plus en détail. Dans cette section, nous allons ainsi premièrement définir le concept d'identité numérique afin de bien recentrer le sujet. Ensuite, nous présenterons les différentes variantes, catégories et architectures possibles des systèmes de gestion de l'identité.

3.2 Le concept d'identité numérique

Pour reprendre les mots de (Cameron 2005, p.1) : « The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception which will cumulatively erode public trust in the Internet ». Il est vite apparu évident qu'il était nécessaire de développer des systèmes permettant d'identifier les utilisateurs sur internet. En effet, il est souvent nécessaire d'identifier les utilisateurs ne serait-ce que pour contrôler les services auxquels ils peuvent avoir accès : « (...) there is often a need to know who the users are and to control what services they are entitled to use » (Jøsang and Pope 2005, p.1)[21]. Dans ce but, des systèmes de gestion d'identité ont été conçus. « An identity is a representation of an entity in a specific application domain » (Jøsang and Pope 2005, p.2)[21]. Cette dernière phrase résume bien ce qu'est une identité. Et l'entité à laquelle nous faisons allusion peut être une personne ou une organisation. En général, une identité ne peut être associée à plus d'une entité, bien qu'il puisse y avoir des "exceptions" puisque, par exemple, nous pourrions avoir une entité "famille" qui correspondrait ainsi à plusieurs personnes. Même dans cette "exception", du point de vue du fournisseur de service, l'identité est finalement liée à une seule entité qu'est la famille, et non les personnes qui en font partie individuellement.

Une identité consiste en un ensemble d'attributs, comme le souligne (Jøsang and Pope 2005, p.2)[21] : « An identity consists of a set of characteristics, which are called identifiers when used for identification purposes. These characteristics may or may not be unique within the identity domain. They can have various properties, such as being transient or permanent, self-selected or issued by an authority, suitable for human interpretation or only by computers. The possible characteristics of an identity may differ, depending on the type of real world entity being identified. For example, a date of birth applies to people, but not to organisations ; a national company registration number applies to a company, but not to a person ». Cela démontre ici la complexité qui se cache dans la gestion

de ces identités. Car au-delà de ces attributs qui diffèrent d'un type d'entité à une autre, mais aussi et surtout d'un domaine à un autre, il arrive que certains domaines permettent plusieurs identités pour une entité. Un exemple serait de considérer une personne ayant à la fois le rôle de parent et d'enseignant dans un système scolaire, et qui aurait alors deux identités. L'image(1) ci-dessous synthétise les liens qu'il peut y avoir entre entités, identités et attributs :

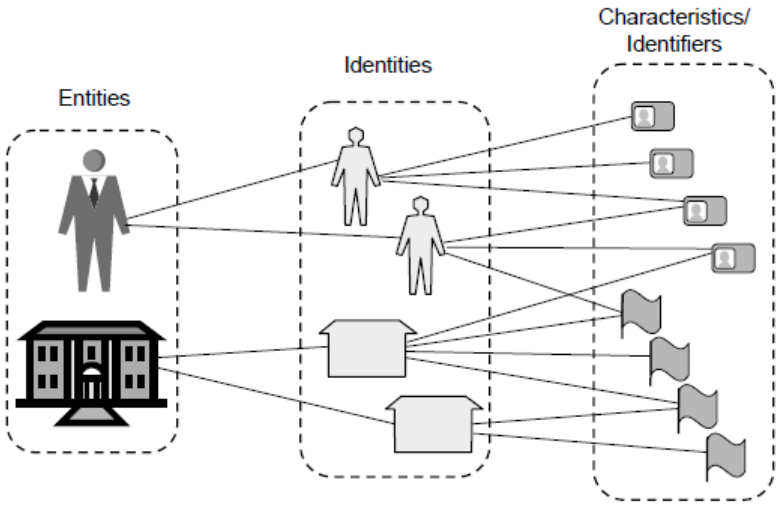

FIGURE 1 – Correspondance entre entités, identités et attributs (Jøsang and Pope 2005, p.3)[21]

« The figure illustrates that an entity, such as a person or an organisation, may have multiple identities, and each identity may consist of multiple characteristics that can be unique or non-unique identifiers » (Jøsang and Pope 2005, p.2)[21].

3.3 Modèles de systèmes de gestion d'identité

Nous allons maintenant parcourir les différentes variantes de système de gestion de l'identité des utilisateurs. Pour ce faire, nous allons nous baser sur le travail de (Jøsang and Pope 2005)[21] : « User Centric Identity Management », dans lequel les systèmes de gestion d'identité ont été catégorisés.

3.3.1 Modèles traditionnels

Il existe diverses variantes de ce que (Jøsang and Pope 2005)[21] appellent des modèles "traditionnels" et nous les décrivons ci-dessous :

Isolé :
Le modèle de gestion d'identité le plus courant, selon (Jøsang and Pope 2005, pp3-4)[21] est le modèle dit d'"utilisateur isolé". Il porte bien son nom puisque dans ce modèle, c'est le fournisseur de service qui remplit tous les rôles de gestion de l'identité. En effet, il est à la fois responsable de l'octroi d'informations d'identification et d'identifiants à ses utilisateurs. Un utilisateur recevra ainsi un identifiant unique de chaque service ou fournisseur d'identité avec lesquels il interagit. Par conséquent, l'utilisateur aura des identifiants séparés pour chacun de ces services également. Ce que nous venons de décrire peut être illustré par le schéma(2) ci-dessous :

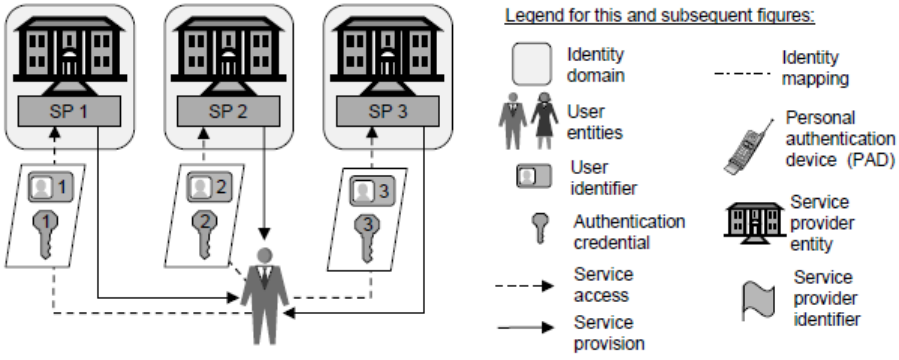

FIGURE 2 – Modèle de l'utilisateur isolé (Jøsang and Pope 2005, p.4)[21]

C'est le genre de modèle qui a purement été pensé du point de vue du fournisseur de service. En effet, cela facilite tous les aspects liés à la gestion des identifiants, car un fournisseur de service n'a à se soucier que de son système et des attributs qui composent ses identifiants. Par contre, cela peut vite devenir ingérable du point de vue de l'utilisateur puisque ce dernier devra retenir et gérer autant d'identifiants que de services avec lesquels il interagit. C'est un problème, comme les auteurs le soulignent : « Users are often required to memorise passwords, which unavoidably leads to users forgetting passwords to infrequently used services. Forgotten passwords, or simply the fear of forgetting, create a significant barrier to usage, resulting in many services not reaching their full potential. For important sensitive services, where password recovery must be highly secure, forgotten passwords can also significantly increase the cost for the service providers » (Jøsang and Pope 2005, p.4)[21]. De plus, par peur d'oublier leur mot de passe, les utilisateurs pourraient être tentés d'utiliser des mots de passe ne respectant pas les règles de sécurité, c'est-à-dire des mots de

passe trop simples ou des mots de passe similaires pour les différents systèmes, ce qui implique alors des problèmes de sécurité.

Fédéré :
Le modèle dit "fédéré" tente quant à lui de palier aux problèmes décrits dans le modèle isolé. Il permet en effet de réduire la quantité d'identifiants à retenir puisqu'il repose sur le fait que des fournisseurs de services se sont regroupés pour accepter les identifiants des uns et des autres : « Identity federation can be defined as the set of agreements, standards and technologies that enable a group of service providers to recognise user identifiers and entitlements from other service providers within a federated domain » (Jøsang and Pope 2005, p.4)[21]. Dans ce modèle, les différents fournisseurs de services d'une fédération ont alors passé des accords entre eux pour qu'une identité du groupe puisse être utilisée dans chacun d'entre eux. Une correspondance doit cependant être maintenue entre les différents identifiants d'un utilisateur afin de pouvoir le reconnaître. Cela peut être illustré par le schéma(3) ci-dessous :

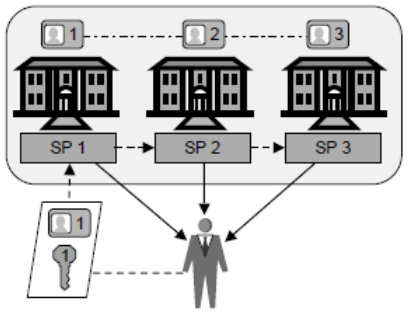

FIGURE 3 – Modèle de l'identité fédérée (Jøsang and Pope 2005, p.4)[21]

Ainsi, quand un utilisateur est authentifié auprès de l'un des fournisseurs, il l'est également pour les autres fournisseurs de la fédération. « This results in a single virtual identity domain » (Jøsang and Pope 2005, p.4)[21]. Ou avec d'autres mots : « The federation of isolated identifier domains gives the client the illusion that there is a single identifier domain. The user can still hold separate identifiers for each service provider. However, he does not necessarily need to know or possess them all. A single identifier and credential is sufficient for him to access all services in the federated domain » (Jøsang and Pope 2005, p.5)[21]. C'est le genre de modèle qui peut être utilisé pour proposer ce qu'on appelle du "Single-Sign-On" (SSO). Toutefois, cela ne règle pas entièrement le problème des identités démultipliées puisque l'utilisateur devra toujours avoir une identité par fournisseur de la fédération, même s'il n'utilise que l'une d'elles pour se connecter : « However, a potential problem is that users will still have to manage multiple identities and credentials, even if they are not actively using all of them » (Jøsang and Pope 2005, p.5)[21].

Centralisé :

Dans cette catégorie, il existe encore trois sous-modèles. Le point commun entre les trois est l'existence d'un fournisseur d'identifiant unique pour tous les fournisseurs de services. Nous décrivons ces sous-modèles ci-dessous :

— **Utilisateur commun :**

La manière la plus simple de centraliser la gestion des identités est de laisser ce travail à une entité séparée qui s'occupe alors de son côté de fournir les identifiants aux utilisateurs, et ce pour tous les fournisseurs de services. Ce modèle peut être représenté par le schéma(4) ci-dessous :

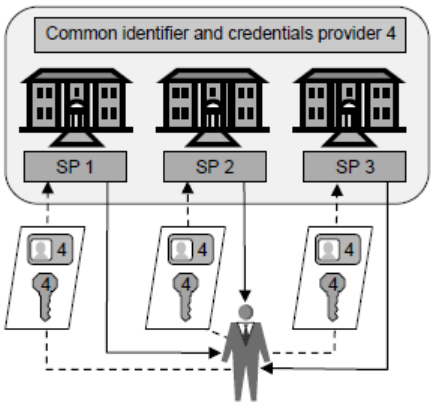

FIGURE 4 – Modèle de l'utilisateur commun (Jøsang and Pope 2005, p.5)[21]

L'utilisateur peut ainsi avoir accès à tous les fournisseurs de services avec le même identifiant.

— **Méta utilisateur :**
Il est possible que les fournisseurs de services partagent des données d'identité à un niveau dit "meta". Cela peut être fait en mettant en commun les attributs identifiants spécifiques à chaque founisseur dans un meta identifiant. Ce modèle peut être illustré par le schéma(5) ci-dessous :

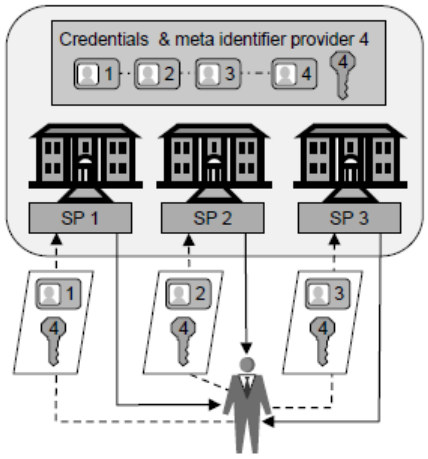

FIGURE 5 – Modèle du méta utilisateur (Jøsang and Pope 2005, p.6)[21]

C'est en général une approche qui est assez populaire dans les grandes entreprises : « The meta identifier approach is commonly implemented by a so-called meta directory, and is a popular approach for integrating legacy identity management systems in large enterprises. In this case, all the services linked to the meta identity domain are usually under the administration of a single organisation or authority » (Jøsang and Pope 2005, p.6)[21]. Ce modèle pourrait aussi être utilisé pour différents fournisseurs de services mais cela nécessiterait des accords quand aux règles relatives à l'identité et une confiance accrue entre les parties impliquées, comme le soulignent les auteurs. Du point de vue de l'utilisateur, c'est un mécanisme qui est en général caché et qui peut être perçu comme une synchronisation entre les différents fournisseurs de services.

— **Single-Sign-On :**
Une fois authentifié auprès d'un fournisseur de service, ce modèle permet à un utilisateur d'être considéré comme authentifié par d'autres fournisseurs de services. Il n'a alors besoin de se connecter qu'une seule fois afin de pouvoir accéder à tous les services. Le modèle Single-Sign-On peut être représenté par le schéma(6) ci-dessous :

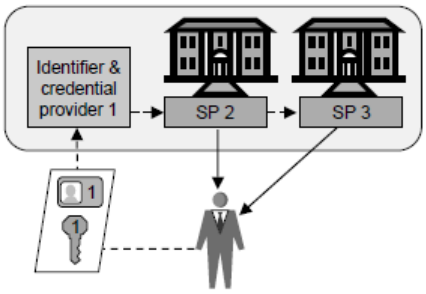

FIGURE 6 – Modèle Single-Sign-On (SSO) (Jøsang and Pope 2005, p.6)[21]

Ce modèle est assez similaire au modèle fédéré si ce n'est que celui ne nécessite pas de correspondance entre les différents identifiants d'un utilisateur puisque, ici, le même est utilisé par chaque fournisseur de service.

3.3.2 Modèle centré sur l'utilisateur

Un solution d'authentification devrait prendre en compte la manière dont les identités et les identifiants sont gérés par les utilisateurs, comme le suggèrent (Jøsang and Pope 2005, p.7)[21]. Un des objectifs principaux à considérer lors du développement d'une telle solution est donc l'utilisabilité. Si cette dernière s'avère être faible, cela aura une conséquence négative sur l'authentification elle-même puisque les utilisateurs ne seront pas en mesure de gérer leurs identifiants de manière adéquate. Il est d'ailleurs intéressant de constater, comme le soulignent (Jøsang and Pope 2005, p.7)[21], que de leur coté les fournisseurs de services ont en général automatisé leur système de gestion de l'identité et d'authentification, tandis que les utilisateurs ont pour la majorité une gestion exclusivement manuelle de leurs identifiants. Une multiplication des identifiants, du point de vue de l'utilisateur, devient vite ingérable.

Parmi les modèles décrits précédemment, le modèle fédéré se distingue par son besoin de simplifier la vie des utilisateurs. L'idée de base étant qu'un utilisateur n'ait besoin que d'une paire identité-identifiants. Il n'est cependant pas concevable de penser qu'il est possible de réunir tous les fournisseurs de services au sein d'une même fédération : « However, it is inconceivable that only one single federation domain will exist, and it is evident that there will never be a single identity domain for all service providers. Also, services with different levels of sensitivity and risk will require different types of credentials » (Jøsang

and Pope 2005, p.7)[21].

Du point de vue de (Jøsang and Pope 2005, p.7)[21], une toute nouvelle approche est nécessaire. Il paraît évident et naturel d'introduire un système de gestion de l'identité du côté de l'utilisateur. La solution serait alors de laisser les utilisateurs stocker les identités et identifiants provenant de différents fournisseurs de services dans un unique périphérique inviolable tel qu'un appareil portable ou une carte à puce. Le nom anglais de ce genre de modèle "user centric" pour "centré sur l'utilisateur" vient du fait que de tels périphériques sont personnels. L'avantage est que ce type de modèle peut être combiné avec n'importe quel modèle précédemment décrit. Le schéma(7) suivant illustre par exemple comment il peut être combiné avec le modèle isolé :

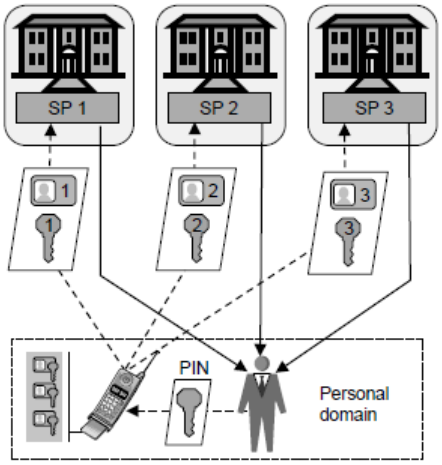

FIGURE 7 – Modèle centré sur l'utilisateur (Jøsang and Pope 2005, p.7)[21]

Il faut noter que ce genre de périphérique doit rester sous le contrôle de l'utilisateur, comme le suggèrent (Jøsang and Pope 2005, p.8)[21], sous peine de tomber dans les mêmes travers qu'auparavant dans le cas où ils seraient gérés par les fournisseurs de services, puisque cela résulterait en une prolifération de ces périphériques.

3.4 Conclusion

Les modèles présentés ci-dessus nous serviront de base à l'analyse de trois projets européens portant sur l'identité numérique plus loin dans ce mémoire. Ils nous permettront de comparer ces derniers d'un point de vue structurel et de tirer des conclusions sur leur choix.

4 Méthodologie d'évaluation

4.1 Introduction

Afin d'analyser les projets de la manière la plus précise possible, il est opportun de dresser une grille d'analyse qui nous permettra d'évaluer chaque projet indépendamment, mais aussi de les comparer les uns aux autres. Dans cette section, nous allons définir cette grille qui nous servira alors à comparer les projets que nous allons analyser dans la section suivante. Nous commencerons par définir chaque élément de la grille en détail et nous finirons en les présentant dans un tableau afin de les synthétiser.

4.2 Présentation de la grille d'analyse

En 2005, Cameron, responsable en charge de gérer l'architecture de l'identité chez Microsoft ("Chief Identity Architect"), a publié un article appelé "The Laws of Identity". Dans celui-ci, il pose notamment une question : "Why is it so hard to create an identity layer for the Internet ?". Question à laquelle il répond lui-même : "Mainly because there is little agreement on what it should be and how it should be run. This lack of agreement arises because digital identity is related to context, and the Internet, while being a single technical framework, is experienced through a thousand kinds of content in at least as many different contexts – all of which flourish on top of that underlying framework. The players involved in any one of these contexts want to control digital identity as it impacts them, in many cases wanting to prevent spillover from their context to any other" (Cameron 2005, p.2)[15]. Cette réponse qu'il apporte dans son article témoigne de l'inexistence d'un standard à proprement parlé en ce qui concerne l'identité numérique. Chaque intervenant (fournisseur de service,...) y allant de son propre chef en proposant des systèmes tous différents les uns des autres. Il est de nos jours capital que les acteurs du secteur fassent évoluer leurs systèmes vers plus de coordination.

Dans son article, Cameron présente sept lois qui, selon lui, expliquent le succès ou l'échec des systèmes d'identité digitale. Pour établir notre grille d'analyse, nous nous baserons d'abord sur les critères qui se dégagent de ces lois. Nous y ajouterons ensuite de nouveaux critères qui, selon nous, sont importants à considérer pour améliorer l'efficacité, la sécurité et la pérennité de ces systèmes.

4.2.1 Cameron : Contrôle et consentement de l'utilisateur

La première loi selon (Cameron 2005, p.6)[15] concerne le consentement de l'utilisateur. Tout système d'identité ne devrait révéler des informations d'identification que si l'utilisateur a donné son consentement. Pour reprendre les mots de (Cameron 2005, p.6)[15] : « The system must first of all appeal by means of convenience and simplicity. But to endure, it must earn the user's trust above all. Earning this trust requires a holistic commitment. The system must be designed to put the user in control - of what digital identities are used, and what

information is released ». Selon l'auteur, le consentement est un élément crucial pour gagner la confiance de l'utilisateur. Et pour ce faire, le système doit "donner les clés" à l'utilisateur afin qu'il ait le contrôle sur les utilisations qui sont faites de ses identités numériques, mais aussi des informations diffusées. L'utilisateur doit aussi, à tout moment, pouvoir être en mesure de savoir à quelles fins ses informations sont collectées. Le système doit également être capable de garantir que les informations iront au bon endroit, et que l'identité de toutes les parties prenantes sont vérifiées. De plus, le système doit renforcer l'idée selon laquelle l'utilisateur a le contrôle quel que soit le contexte.

4.2.2 Cameron : Divulgation minimale et usage limité

La deuxième loi développée par (Cameron 2005, pp6-7)[15] concerne la divulgation minimale de données et la limitation de leurs usages. Selon cette deuxième loi, les données collectées devraient toujours être minimales et destinées à un usage précis. C'est tout d'abord important pour limiter les risques de fuite (Cameron 2005, pp.6-7)[15] : « We should build systems that employ identifying information on the basis that a breach is always possible. Such a breach represents a risk. To mitigate risk, it is best to acquire information only on a "need to know" basis, and to retain it only on a "need to retain" basis ». Mais, de plus, un système qui stocke moins de données d'identification possible devient une cible moins attrayante pour les nn vols d'identité. En se basant sur le principe "need to know" précédemment cité, il n'y a plus la possibilité de récolter des données et de les garder "au cas où" elles deviendraient nécessaires ou utiles à un moment donné (Cameron 2005, p.7)[15]. Cameron donne un exemple selon lequel il est même possible de dériver une donnée afin de ne pas la stocker directement. Ainsi, si un certain âge est requis, il sera préférable de stocker la catégorie de l'âge plutôt que la date de naissance de l'individu. Cette dernière pouvant plus précisément identifier une personne qu'une catégorie d'âge. Pour reprendre les mots de (Cameron 2005, p.7)[15] : « We can also express the Law of Minimal Disclosure this way : aggregation of identifying information also aggregates risk. To minimize risk, minimize aggregation ».

4.2.3 Cameron : Tiers légitimes

Selon la troisième loi de (Cameron 2005, pp7-8)[15], il est impératif que le système fasse savoir à l'utilisateur les systèmes tiers avec lesquels il interagit lorsqu'il partage des données. C'est un pré-requis qui doit être applicable aussi bien pour l'utilisateur qui émet les données d'identification que pour les tiers qui les consomment. Cela afin d'assurer que l'utilisateur donne son consentement en toute connaissance de cause. Il ne peut y avoir aucun tiers caché dans un partage de données d'identification. C'est une base nécessaire pour que les systèmes puissent gagner la confiance de leurs utilisateurs : « (...) the system must be predictable and "translucent" in order to earn trust. (...) In the physical world we are able to judge a situation and decide what we want to disclose about ourselves. This has its analogy in digital justifiable parties », selon (Cameron

2005, pp7-8)[15]. Aussi, chaque partie faisant partie du partage de données doit fournir aux autres une déclaration de politique sur l'utilisation qui sera faite des données partagées, si partage il y a : « Every party to disclosure must provide the disclosing party with a policy statement about information use » (Cameron 2005, p.8)[15].

4.2.4 Cameron : Identité dirigée

La quatrième loi de (Cameron 2005, pp8-9)[15] suggère qu'un système universel d'identité doit supporter ce qu'il appelle des identités "omnidirectionnelles", destinées à être utilisées par des entités publiques, et des identités "unidirectionnelles", qui, elles, seront destinées à des entités privées. L'auteur utilise le terme "omnidirectionnelle" pour désigner une identité qui a pour vocation à être dévoilée au plus grand nombre, à des fins de découvrabilité. Nous pouvons voir cela comme une sorte d'étiquette, ou de "balise" pour reprendre le terme utilisé par l'auteur, permettant aux autres entités d'avoir un aperçu de son identité. Il utilise le terme "unidirectionnelle" pour, au contraire, désigner une identité très privée qui ne sera utilisée qu'entre son propriétaire et le système avec lequel elle a été définie. Entamer une relation avec un autre système implique de devoir définir une toute autre (et indépendante) identité unidirectionnelle.

4.2.5 Cameron : Pluralisme d'opérateurs et de technologies

La cinquième loi énoncée par (Cameron 2005, p.9)[15] requiert qu'un système universel d'identité soit en mesure de faire fonctionner de multiples technologies d'identité, elles-mêmes maintenues par de multiples fournisseurs d'identité. En effet, nous avons vu que par la multitude de contextes, et ainsi de systèmes d'identité qui en découlent, il n'en existe pas qui serait capable d'être valable pour tous ces contextes. Aussi, aucun fournisseur d'identité ne peut alors convenir à tous les contextes. C'est pour contrer ces lacunes qu'un système candidat devra garantir qu'il permet le fonctionnement de divers systèmes de gestion d'identité, eux-mêmes gérés par différents fournisseurs.

4.2.6 Cameron : Intégration humaine

La sixième loi de (Cameron 2005, p.10)[15] suggère que les systèmes d'identité doivent considérer l'utilisateur comme composant à part entière du système. Cela se traduit par la mise à disposition de mécanismes de communication homme-machine sans aucune ambiguïté offrant une protection contre les attaques visant l'identité. L'auteur mentionne le fait que jusqu'à maintenant, les communications entre serveurs web et les navigateurs sont bien sécurisées grâce à l'utilisation de moyens cryptographiques. Le problème réside alors au niveau de l'utilisateur lui-même : « We have done a pretty good job of securing the channel between web servers and browsers through the use of cryptography – a channel that might extend for thousands of miles. But we have failed to adequately protect the two or three foot channel between the browser's display and the

brain of the human who uses it. This immeasurably shorter channel is the one under attack from phishers and pharmers » (Cameron 2005, p.10)[15]. Le but est donc de fournir une expérience utilisateur ne laissant pas de place à l'ambiguïté mais bien à des actions prévisibles et claires pour permettre des décisions informées : « This concept calls for profoundly changing the user's experience so it becomes predictable and unambiguous enough to allow for informed decisions » (Cameron 2005, p.10)[15].

4.2.7 Cameron : Expérience cohérente dans tous les contextes

Dans son document, (Cameron 2005)[15] parle d'un nombre assez conséquent de ce qu'il appelle des "contextes". Typiquement, ce sont les entités avec lesquelles il est possible d'interagir via internet. Il va sans dire qu'il en existe énormément et cela implique qu'il en résulte un nombre au moins égal de manières de gérer l'identité, puisque chaque "contexte" veut la contrôler de la façon dont il en a besoin. Cette septième et dernière loi de (Cameron 2005, pp10-11)[15] propose que les méta-systèmes d'identité garantissent une expérience simple et cohérente tout en séparant les contextes au travers de divers opérateurs et technologies. Pour cela, ces systèmes devraient permettre à l'utilisateur de pouvoir choisir l'identité à utiliser pour un contexte donné, ce qui permettra à l'utilisateur de contrôler ce qui est partagé, et ce de la même manière et avec la même interface pour tous les contextes : « As users, we need to see our various identities as part of an integrated world which none the less respects our need for independent contexts » (Cameron 2005, p.11)[15].

4.2.8 Authenticité de l'identité

A une époque où les faux papiers et les faux profils sont une réalité, il va de soi qu'il doit être possible d'attester de l'authenticité d'une identité numérique. Nous devons pouvoir certifier qu'une personne ayant créé un profil est réellement celle qu'elle prétend être, et que les informations qui y sont rassemblées sont authentiques. Ainsi, tout système d'identification devrait s'assurer que lorsqu'un nouveau compte est créé, il identifie une personne unique et qu'il s'agit effectivement de la personne renseignée, ou en d'autres termes, de l'authenticité de l'identité fraîchement créée. Il semble évident qu'un individu facilement identifiable ne voudra, en principe, commettre de délit ou de fraude sur quelque plateforme que ce soit si son identité est connue. Une méthode de vérification consisterait à vérifier que l'individu est détenteur de documents officiels portant son identité. Cela peut être une carte d'identité, un permis de conduire, ou tout autre document attestant de l'identité de la personne. Le succès de ce critère reposera dans la capacité du système d'identification à vérifier que la personne présentant un document officiel est bien cette personne, mais aussi à vérifier que le document présenté est lui-même authentique. Car nous pourrions encore envisager qu'une personne crée un compte ou un profil avec un document trouvé, volé ou falsifié. Ce critère n'aura donc aucune valeur si le système n'est pas en mesure de s'assurer de l'identité du porteur et de l'authenticité du document

présenté lors de la création du compte ou du profil.

4.2.9 Contrôle des autorités

La cybercriminalité fait de nos jours partie de l'actualité, c'est indéniable. Vol d'identité, arnaques en tout genre, phishing (...) internet n'est pas un "monde" sans risque. Nous pensons qu'il est important que les autorités publiques soient impliquées dans la régulation de ces systèmes. Ce contrôle peut prendre deux formes. Il peut, d'une part, être effectué en amont, c'est-à-dire à la création de l'identité et à son émission. En Belgique par exemple, l'émission de nouvelles cartes d'identités est fortement surveillée et c'est un processus effectué par les autorités publiques. D'autre part, il peut s'effectuer en aval, lors d'un litige par exemple. Dans ce deuxième cas, les autorités devraient être en mesure d'effectuer un travail d'investigation poussé et précis afin de pouvoir statuer sur les conflits entre utilisateurs (suite à une fraude, une arnaque,...). Le commerce en ligne dépasse maintenant très souvent nos frontières et il sera également important que les litiges transfrontaliers puissent être résolus.

4.2.10 Sécurisation des données

En parallèle au critère précédent concernant le contrôle des autorités, il est important de se soucier de la sécurisation des données d'identité. Ainsi, nous porterons une grande attention à la manière dont les données sont véhiculées et stockées. Car nous avons beau vouloir créer une interface claire et non-ambiguë pour les utilisateurs afin que ceux-ci puissent être identifiables sur les réseaux, cela deviendra vite inutile si les données d'identité stockées sur le méta-système de gestion d'identité sont vulnérables au vol, et ce quelle que soit la manière. Ainsi, afin d'empêcher les phénomènes d'usurpation d'identité, il faudra s'assurer que le système s'appuie sur une sécurité suffisante des données pour prévenir toute attaque.

4.3 Conclusion et synthèse de la grille d'analyse

La grille(8) ci-dessous reprend, en guise de synthèse, les critères qui seront utilisés pour évaluer les différents projets portant sur l'identité numérique. Pour chaque projet, nous allons analyser la manière dont ceux-ci répondent à ces critères et ce afin d'évaluer leur potentiel respectif dans la consolidation de la confiance sur les plateformes de l'économie collaborative.

Grille d'analyse		
#	Critères	Caractéristiques
1	Contrôle et consentement de l'utilisateur	Un système d'identité ne devrait pouvoir révéler des informations identifiant l'utilisateur qu'avec le consentement de ce dernier.
2	Divulgation minimale et usage limité	Divulgation minimale et usage limité & La solution qui divulgue le moins de données d'identification et qui limite au mieux les usages de ces dernières sera la solution la plus stable à long terme.
3	Tiers légitimes	Les systèmes d'identité digitale doivent être conçus pour ne divulguer des informations qu'aux tiers ayant un besoin justifiable au sein d'une relation d'identité.
4	Identité dirigée	Le système d'identité digitale doit pouvoir supporter aussi bien des identifiants "omnidirectionnels" (publiques) et "unidirectionnels" (privés).
5	Pluralisme d'opérateurs et de technologies	Un système universel d'identité doit pouvoir fonctionner avec de multiples technologies d'identité et de multiples fournisseurs d'identité.
6	Intégration humaine	Le système universel d'identité doit considérer l'utilisateur comme composant à part entière système en fournissant des interfaces non-ambiguës offrant une protection contre les attaques visant l'identité.
7	Expérience cohérente dans tous les contextes	La solution candidate doit être en mesure de fournir une expérience homogène et cohérente à ses utilisateurs malgré la multitude des contextes.
8	Authenticité de l'identité	Le système universel d'identité doit être capable de garantir l'authenticité des informations d'identité fournies. Si elles sont supposées identifier un individu ou une entité, elles doivent être authentifiables.
9	Contrôle des autorités	Un contrôle doit être opérable par les autorités publiques, que ce soit en amont ou en aval à l'émission d'une nouvelle identité officielle.
10	Sécurisation des données	Les échanges et le stockage des données d'identification doivent être sécurisés pour empêcher les phénomènes d'usurpation.

FIGURE 8 – Grille d'analyse

5 Analyse de 3 projets

5.1 Introduction

Dans cette section, nous allons parcourir en détail trois projets européens (ARIES[7], STORK 2.0[8] et OLYMPUS[3]) portant sur l'identité numérique. Nous avons choisi d'analyser ces trois projets après avoir trouvé STORK 2.0 lors de nos recherches pour réaliser l'état de l'art sur les mécanismes de construction de la confiance. En cherchant un peu plus loin, nous avons de fil en aiguille trouvé les projets ARIES et OLYMPUS qui s'avèrent également être des projets centrés sur l'identité digitale et financés en partie par l'union européenne. Ces projets ont des approches différentes et ne fournissent pas tous les mêmes fonctionnalités. Ils sont également différents en terme d'architecture. Afin de les comparer de la manière la plus adéquate, nous allons les confronter à la grille d'analyse développée dans la section précédente. Nous allons ainsi, pour chaque projet, faire une présentation, enchaîner avec leur statut (au moment de l'écriture de ce document), et nous poursuivrons ensuite avec le fonctionnement et l'architecture pour enfin les évaluer sur base de la grille d'analyse développée au chapitre précédent. Sur base des résultats de l'analyse d'un projet, il sera alors possible de déterminer des pistes d'amélioration pour lui-même et éventuellement pour les projets futurs, sous forme de recommandations. En guise de conclusion à cette section, une grille récapitulative sera fournie, reprenant les différents critères et les résultats observés en analysant les projets.

5.2 ARIES

5.2.1 Introduction au projet

Le projet ARIES, pour "reliAble euRopean Identity EcoSystem", est un projet qui a démarré en septembre 2016 et a reçu un financement de la commission européenne, dans le cadre de ce qui est appelé le : "EU Framework Programme for Research and Innovation HORIZON 2020", pour un montant total d'environ 2,2 millions d'euros[7]. Il a été conduit par un ensemble d'entités (comprenant des entreprises, des universités, la police fédérale belge,...) et coordonné par la société ATOS. Le projet ARIES a pour ambition de fournir une solution solide, fiable, conviviale ainsi que des processus d'authentification efficaces tout en respectant pleinement l'utilisateur et en garantissant la protection et la confidentialité de ses données personnelles (Bernal Bernabe, Torres Moreno, Martin, Crespo, Skarmeta, Fortune, Lodge, Oliveira, Silva, Martin, Valero et Alamillo 2019, p.2)[14]. Le projet vise à palier à la vulnérabilité des identités individuelles dans un monde qui devient de plus en plus digital, et où la cybercriminalité sévit chaque jour. Le projet a ainsi pour finalité de combler un "vide" au niveau d'une approche transfrontalière de l'identité numérique, puisque selon (Bernal Bernabe, Torres Moreno, Martin, Crespo, Skarmeta, Fortune, Lodge, Oliveira, Silva, Martin, Valero et Alamillo 2019, p.2)[14] : « (...) there is not a common approach in Europe (from the point of view of the legislation, cross-border cooperation and policies) to address identity-related crimes. This situation costs

billions of Euros to countries and citizens in fraud and theft ».

Avec l'écosystème proposé par le projet ARIES, les utilisateurs seront en mesure de créer une identité numérique liée à une identité physique (telle qu'un passeport ou une carte d'identité électronique) grâce à la biométrie tandis que les informations d'inscription seront stockées dans un "coffre-fort" sécurisé uniquement accessible par les autorités en cas d'incident. Ils seront également capables de dériver des "sous-identités" présentant divers attributs d'identité en fonction des besoins.

Les objectifs du projet peuvent être résumés de la sorte : « ARIES main goal is to deliver a comprehensive framework for reliable e-identity ecosystem comprising new technologies, processes and security features that ensure highest levels of quality in eID based on trustworthy security documents and biometrics for highly secure and privacy-respecting physical and virtual identity management, with the specific aim to tangibly achieve a reduction in levels of identity theft, fraud and associated crimes. The set of solutions will be designed to achieve required levels of multi-party trust with efficiency, ease of adoption and convenience for all end-users (citizens, law enforcement, businesses), consolidating Europe as world leader in enhanced identity-based services as a basis to boost the competitiveness of its economy »[7].

5.2.2 Statut du projet

Le projet s'est terminé au bout de trente mois en février 2019 sur une note positive puisque des tests ont été réalisés pour démontrer l'utilisabilité de l'écosystème ARIES ainsi que ses performances dans l'exécution des tâches qui étaient attendues dans différents contextes d'usage. Selon (Bernal Bernabe, Martin, Torres Moreno, Cordero, Bahloul and Skarmeta 2019, p.22)[13] : « The results proved feasibility and applicability to manage efficiently privacy-preserving, and user-friendly manner user's virtual identities in different contexts. Small scale pilots has demonstrated successfully new approach to web authentication and replacement of traditional boarding pass and passports/documents by a virtual credentials kept securely in mobile devices, while respecting his privacy and maintaining performance authentication with biometric times. Moreover, the duty-free use case has shown the Aries' benefits for user's to preserve their privacy in face-to-face and mobile authentication scenarios, revealing minimal information when Zero Knowledge Proofs were used instead of user's attributes in plaintext ». Comme le mentionnent en effet (Bernal Bernabe, David, Torres Moreno, Cordero, Bahloul and Skarmeta 2019, p.2)[13], le projet ARIES a été déployé, validé et testé avec succès dans deux projets pilotes : « The first one is related to online eCommerce transactions that requires strong authentication and high level of assurance and trust using face recognition techniques with mobiles, whereas the second scenario is intended to reinforce the current face-to-face identity management processes, such as airport user journey. The airport scenario demonstrates the Aries capabilities to replace physical eIDs with mobiles in certain processes, for instance allowing self-boarding in the plane with the highest Level of Assurance using dedicated boarding cameras, combining

face recognition and mobile PKIs technologies with virtual identities originally derived from official physical eIDs. It also shows the capabilities to strengthen user's privacy revealing the minimal amount of personal information (e.g. demonstrating certain predicates over personal attributes using Zero Knowledge Proofs) in face-to-face digital purchases inside the airport, through the Aries App ». Comme décrits par (Bernal Bernabe, David, Torres Moreno, Cordero, Bahloul and Skarmeta, pp13-15)[13], les scénarios sur lesquels le projet a été testé sont les suivants :

— **Scénario e-commerce :**
Le scénario du e-commerce est basé sur un des cas les plus fréquents d'utilisation d'identité virtuelle. Un client sera connecté à un fournisseur de service, dans ce cas-ci, un site de commerce en ligne, pour acheter un bien en utilisant son identité virtuelle et en partageant des informations personnelles. Puisque la transaction est en ligne, elle ne nécessite aucune intervention humaine et le processus est donc vulnérable à l'usurpation d'identité.

Pour accomplir ce scénario, quelques étapes sont nécessaires :
- L'utilisateur et le site d'e-commerce doivent tous les deux être inscrits au système ARIES.
- La création d'une identité virtuelle destinée au site d'e-commerce.
- Vérification mutuelle des identités virtuelles.
- Établissement d'un accord sur les attributs à présenter.
- Authentification biométrique du client.
- Sélection des attributs spécifiques de l'utilisateur à partager avec le site, et connexion de l'utilisateur au site d'e-commerce.

Trois acteurs sont impliqués dans ce scénario :
- L'utilisateur (le client).
- Le site d'e-commerce.
- Le système de gestion d'identité (ARIES).

L'exécution de ce scénario s'effectue alors en deux phases :
- **Phase 1 :**
  En premier lieu, la création d'une identité virtuelle qui permettra aux utilisateurs de générer une ou des identité(s) virtuelle(s) mobile(s) dérivée(s) de documents officiels de manière sécurisée. Concrètement, une identité virtuelle dans l'écosystème ARIES est une identité contenant les attributs strictement nécessaires, et qui est liée simultanément à un attribut biométrique et un document physique d'identité tel un passeport ou une carte d'identité. Elles sont stockées et gérées au moyen d'un "portefeuille" sécurisé installé en général sur le smartphone de l'utilisateur.
- **Phase 2 :**
  C'est pendant cette phase que la vérification des informations d'identification de l'utilisateur et que le lien entre cette identité client avec le compte existant dans la base de données du commerce en ligne ont lieu. Pendant cette phase d'authentification, ARIES génère un QR code comme moyen de "communication" entre l'application mobile

ARIES et le site afin d'éviter toute soumission de nom d'utilisateur, ce qui améliore l'utilisabilité et accélère l'expérience. L'utilisateur doit alors sélectionner une identité dans son "portefeuille" mobile, lire le QR code sur la page du e-commerce au moyen de son téléphone et sélectionner dans l'application tout attribut supplémentaire requis à partager pour la connexion.

Le processus de ce scénario peut être résumé par le schéma(9) ci-dessous :

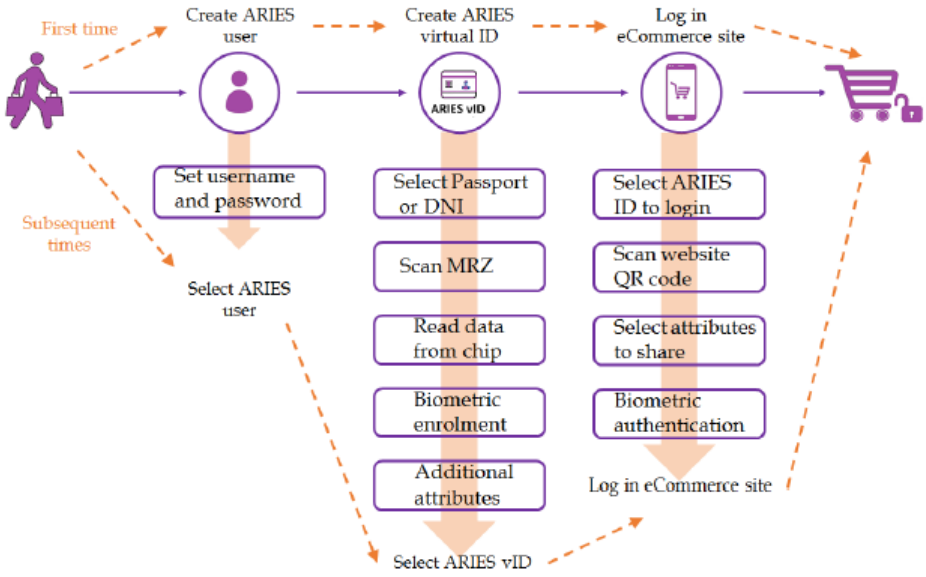

FIGURE 9 – ARIES : e-commerce scenario (Bernal Bernabe, Martin, Torres Moreno, Cordero, Bahloul and Skarmeta 2019, p.14)[13]

— **Scénarios de l'aéroport :**

Le scénario de l'aéroport est divisé en deux sous-scénarios : le premier concerne l'embarquement, le second les achats dans les boutiques de l'aéroport :

— **Embarquement :**

Le scénario d'embarquement démontre l'utilisation d'une identité virtuelle ARIES dans le contexte d'un contrôle d'accès physique où il est nécessaire d'avoir une identification forte et efficace.

La première étape est sensiblement la même que dans le scénario du site d'e-commerce : elle consiste en la vérification de l'identité virtuelle. Les attributs partagés contiennent uniquement les informations nécessaires pour vérifier que l'individu est bien le propriétaire du pass d'embarquement et une vérification biométrique (reconnaissance faciale ou vocale) est nécessaire pour cette étape, puisque l'identité

virtuelle, en plus d'être liée à un document officiel, est aussi liée à un attribut biométrique. En utilisant le pass d'embarquement, un dérivé d'identité ARIES et un attribut biométrique, le terminal d'embarquement doit valider toutes les données pour démontrer l'identité de l'individu. Pour ce faire, un scan biométrique est effectué et comparé au service de vérification biométrique. Une fois la vérification faite, l'individu est identifié.

— **Boutique d'aéroport :**
Dans ce scénario, l'utilisateur désire acheter certains biens à l'accès restreint, comme l'alcool, dans un magasin de l'aéroport et veut que sa vie privée soit respectée. En utilisant l'écosystème ARIES, l'utilisateur peut effectuer son achat d'une manière simple. En premier lieu, il s'authentifie dans le magasin grâce à ARIES en présentant son pass d'embarquement avec le QR code. Ensuite, le vendeur peut vérifier de manière confidentielle, grâce à ARIES, que l'individu qui souhaite effectuer l'achat du bien restreint soit conforme aux exigences. En l'occurrence, pour acheter de l'alcool, qu'il soit âgé d'au moins 18 ans. ARIES se conforme au principe de divulgation minimale de sorte que ni le magasin, ni le vendeur n'aient besoin ou la possibilité de collecter des informations supplémentaires. Cela signifie que la boutique ne peut obtenir aucune information personnelle de l'utilisateur au-delà du minimum requis. Seuls l'assurance que l'utilisateur détient un pass d'embarquement valide et l'âge minimum requis sous forme de fourchette ($>$ 18 ans) peuvent, dans ce scénario, être vérifiés par la boutique. Des documents physiques ne sont ainsi plus nécessaires pour démontrer l'âge.

Bien que le projet ait été un succès dans le sens où les scénarios ont été validés, il demeure un projet pilote et nous n'avons trouvé aucune trace d'une quelconque implémentation 'dans le monde réel'. Néanmoins, le projet a reçu des retours positifs des utilisateurs ayant participé aux tests, selon les résultats[9] : « Les utilisateurs ont apprécié les performances générales de l'application mobile ARIES et ont accueilli positivement l'idée de disposer d'un double moyen numérique pour prouver leur identité ».

5.2.3 Fonctionnement et/ou architecture du projet

Afin de donner un maximum de contrôle à l'utilisateur, les architectes de l'écosystème ARIES on fait le choix d'adopter un modèle d'identité digitale centré sur l'utilisateur. Les processus d'authentification seront alors assurés par un périphérique (tel un smartphone), permettant ainsi l'utilisation d'attributs biométriques (en l'occurrence les reconnaissances faciale et vocale). « L'écosystème numérique proposé vise à renforcer le lien entre les identités physiques et numériques, tandis que sa conception tient compte à la fois des lignes directrices sur la protection de la vie privée et de l'analyse des services existants et des processus de gestion des identités »[9].

L'écosystème ARIES peut être représenté par le schéma(10) ci-dessous :

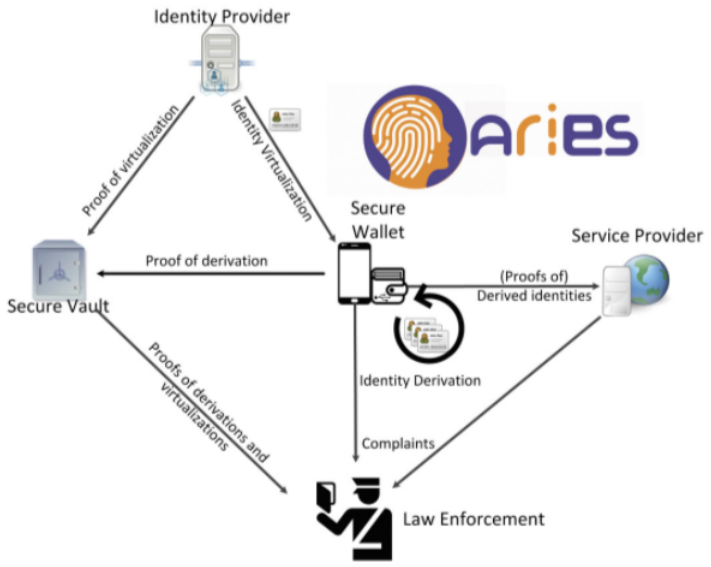

FIGURE 10 – ARIES : ecosystem (Notario, Skarmeta, Bernal Bernabe, Canovas Sanchez and Crespo 2017, p.1)[27]

Les différents éléments qui le composent sont décrits ci-après, à l'aide du travail fourni, notamment, par (Bernal Bernabe, Martin, Torres Moreno, Cordero, Bahloul and Skarmeta 2019)[13] :

— **Secure Wallet :**
Le portefeuille sécurisé (Secure Wallet) désigne l'endroit dans lequel seront stockées les identités virtuelles. Il est en général installé sur le smartphone de l'utilisateur (application ARIES).

— **Secure Vault :**
Le coffre-fort sécurisé (Secure Vault) est un service distribué qui conserve les preuves cryptées des correspondances d'ID, actions et logs collectés toutes les phases du cycle de vie de l'identité que sont la vérification d'identité, l'inscription biométrique et l'utilisation des identités virtuelle. Ce processus de "logging" se fait néanmoins avec le consentement de l'utilisateur concerné. Il met à disposition une API, permettant de créer, lire, modifier et supprimer les données stockées pour un utilisateur. Il supporte également la gestion de la délégation et du contrôle d'accès pour permettre l'accès aux autorités (et uniquement aux autorités) en cas de cybercriminalité. Le cas échéant, les autorités ont alors les droits d'inspecter les logs des transactions stockées dans le coffre-fort et de désanonymiser l'identité de l'utilisateur concerné ainsi que les logs qui y

sont liés. Quand une action est perpétrée sur l'un des composants ARIES, un évènement est enregistré dans le coffre-fort sécurisé.

— **Identity Provider :**
Peuvent être intégrés avec ARIES ou être non-ARIES.

— **Service Provider :**
Le fournisseur de service (Service Provider) n'est autre que le service auquel l'utilisateur désire accéder. Dans le scénario de l'e-commerce, par exemple, cela désigne le site en question.

— **Law Enforcement :**
Les forces de l'ordre (Law Enforcement) ne sont autres que les autorités ayant les compétences d'agir en cas de cybercriminalité. Ces derniers ont alors, dans ce dernier cas, accès au portefeuille sécurisé et à des fonctions de désanonymisation à des fins d'investigations.

Il convient également de décrire la manière dont les processus s'effectuent. Ainsi, nous allons ci-dessous décrire les processus liés au scénario pilote de l'e-commerce, repris au schéma(9). Nous nous focalisons intentionnellement sur le scénario de l'e-commerce puisque c'est pour l'étude des mécanismes propices à la construction de la confiance sur ces plateformes que nous réalisons ce mémoire. Nous considérons, pour nos explications, que c'est la première fois qu'un utilisateur effectue le flux afin de passer à travers toutes les étapes :

1. **Create ARIES user :**
   — **Set username and password :**
   C'est la première étape par laquelle l'utilisateur doit passer quand il veut utiliser l'écosystème ARIES. Cette étape consiste en la création d'un utilisateur ARIES, au moyen d'un nom d'utilisateur et d'un mot de passe.

2. **Create ARIES virtual ID :**
   L'ensemble de sous-étapes ci-dessous permet la création d'une identité virtuelle dérivée d'un document d'identité physique officiel tel un passeport ou une carte d'identité.
   — **Select Passport or DNI :**
   Cette première sous-étape consiste à sélectionner le document physique à importer dans l'application ARIES.
   — **Scan MRZ :**
   La deuxième sous-étape concerne le scan MRZ (pour Machine-Readable Zone), qui consiste à lire une ou des zone(s) du document d'identité afin d'en reconnaître le contenu, avec une technologie OCR (pour Optical Character Recognition). À partir des caractères lus, le système est en mesure de générer la clé d'accès nécessaire pour ouvrir un canal NFC (pour Near Field Communication) sécurisé entre l'appareil mobile et la carte physique utile à l'étape suivante.
   — **Read data from chip :**
   Maintenant que le canal NFC sécurisé a été ouvert à l'étape précédente, le système est capable d'obtenir les informations stockées dans la puce du document physique. Pour cela, la puce génère et envoie un

nombre aléatoire à l'antenne de l'appareil mobile. Ce dernier encrypte ce nombre en utilisant la clé d'accès générée à l'étape précédente et renvoie le résultat à la puce. Ainsi, elle peut vérifier que le nombre a été encrypté avec la bonne clé d'accès et permet ainsi à l'appareil mobile de lire les données de la puce.

- **Biometric enrolment :**
  Cette étape est requise car l'écosystème ARIES a été conçu pour être une plateforme multi-fournisseurs. Après une vérification d'identité, l'attribut biométrique lié doit être vérifié. Deux attributs biométriques sont supportés :
  - Reconnaissance faciale.
  - Reconnaissance vocale.
- **Additional attributes :**
  Durant cette dernière sous-étape de la création d'une identité virtuelle, l'utilisateur choisit des attributs d'identité supplémentaires qu'il désire ajouter à l'identité virtuelle en court de création

3. **Log in eCommerce site :**
   Afin de se connecter au site de e-commerce, l'utilisateur doit réaliser les sous-étapes ci-dessous :
   - **Select ARIES ID to login :**
     Premièrement, l'utilisateur choisit
   - **Scan website QR code :**
     Le site génère alors un QR code à l'aide du système ARIES. L'utilisateur lit le QR code avec son appareil mobile afin de s'authentifier.
   - **Select attributes to share :**
     L'utilisateur sélectionne maintenant les attributs qu'il accepte de partager.
   - **Biometric authentication :**
     Au moyen de l'application mobile ARIES, une vérification biométrique est effectuée, en prenant pour base celle qui est liée à l'identité virtuelle choisie.

5.2.4 Analyse sur base de la grille d'analyse

Contrôle et consentement de l'utilisateur :
Le projet ARIES est complètement conforme à ce critère, selon la page officielle du projet[9] : « Les questions d'éthique sont cruciales pour toute forme de gestion des données et elles ont fait l'objet d'une recherche active dans le cadre du projet. (...) les identités sont uniquement délivrées avec le consentement explicite et informé de l'utilisateur ». En effet dans l'utilisation de l'application ARIES, le consentement de l'utilisateur est explicitement nécessaire à l'exécution des processus d'authentification et de partage de données d'identification.

Divulgation minimale et usage limité :
Le projet répond également à ce critère, comme le soulignent (Bernal Bernabe,

Torres Moreno, Martin, Crespo, Skarmeta, Fortune, Lodge, Oliveira, Silva, Martin, Valero et Alamillo 2019, p.9)[14] : « ARIES focussed on how to optimise the potential for minimising and averting unintended misappropriation and disproportionate use of information for unknown and diverse purposes to which citizens have not explicitly consented ». C'est une information que corrobore le site officiel du projet ARIES : « Nous avons traité la question de l'éthique en veillant à ce qu'aucunes données autres que celles spécifiquement nécessaires au service envisagé ne soient saisies ou collectées à partir du document fourni par l'utilisateur ». C'est également un aspect qui a pu être constaté lors de l'exécution du scénario de la boutique d'aéroport, lorsque que l'utilisateur désire acheter un produit dont l'âge minimum requis est de 18 ans. La vérification se fait alors uniquement avec la preuve que l'utilisateur se trouve bien dans une fourchette d'âge supérieure à l'âge requis, en l'occurrence 18 ans.

Tiers légitimes :
Dans le cadre du projet ARIES, ce critère est discutable. Nous considérons que, lors d'un accès à un site d'e-commerce, seul ce dernier doit en être au courant. Or, en plus du fournisseur de service, le fournisseur d'identité ARIES est lui aussi au courant. Cela ne pose pas de souci lorsque le fournisseur d'identité ARIES se trouve dans le même contexte/domaine que le fournisseur de service, cependant nous n'avons pas trouvé dans l'examen des rapports ARIES d'éléments selon lesquels un consentement est requis lorsqu'un fournisseur d'identité externe au contexte du fournisseur de service est utilisé. Nous émettrons par conséquent quelques réserves quant à ce critère.

Identité dirigée :
Compte tenu de la littérature que nous avons parcourue, et de l'analyse qui a été faite de l'architecture du projet ARIES, nous n'avons pas été en mesure de trouver des informations nous permettant d'affirmer que le projet répond favorablement à ce critère. Par conséquent, nous considérons qu'ARIES ne répond pas à ce critère. Pour rappel, selon (Cameron 2005, pp8-9), un système universel d'identité doit supporter ce qu'il appelle des identités "omnidirectionnelles", destinées à être utilisées par des entités publiques, et des identités "unidirectionnelles", qui, elles, seront destinées à des entités privées. L'auteur utilise le terme "omnidirectionnelle" pour désigner une identité qui a pour vocation à être dévoilée au plus grand nombre, à des fins de découvrabilité, un peu comme l'URL d'un site web.

Pluralisme d'opérateurs et de technologies :
ARIES a été conçu pour permettre aux fournisseurs de services d'avoir des alternatives quant au fournisseur d'identité à utiliser. Ils peuvent ainsi directement authentifier l'identité de l'utilisateur (par exemple en validant un certificat), mais peuvent aussi rediriger la requête à un fournisseur d'identité d'un autre domaine auquel il fait confiance, incluant un opérateur mobile, une banque ou une autorité gouvernementale pour l'authentification mobile d'une identité digitale.

De plus, les fournisseurs d'identité peuvent être interconnectés en s'appuyant sur l'interopérabilité fédérée, permettant ainsi la délégation de l'authentification (par exemple en utilisant STORK). L'interaction avec les fournisseurs d'identité non ARIES peuvent également être réalisée en les contactant via des protocoles standard tels que SAML, OAuth,...(Bernal Bernabe, Torres Moreno, Martin, Crespo, Skarmeta, Fortune, Lodge, Oliveira, Silva, Martin, Valero et Alamillo 2019, p.4)[14]

Intégration humaine :
Cette règle suggère que les systèmes d'identité mettent à disposition des utilisateurs une interface claire et non-ambiguë. ARIES s'utilise au moyen d'une application mobile, sur smartphone. C'est un moyen commode de nos jours pour effectuer des opérations rapidement. Par exemple, beaucoup de personnes effectuent maintenant ses virements bancaires via un smartphone. De plus, les rapports ARIES[9] soulignent ceci : « Les utilisateurs ont apprécié les performances générales de l'application mobile ARIES et ont accueilli positivement l'idée de disposer d'un double moyen numérique (le passeport et la carte d'identité nationale) pour prouver leur identité. L'approche centrée sur l'utilisateur leur a donné l'impression d'avoir le contrôle de leurs données à toutes les étapes ». Nous pourrions ainsi croire que le projet ARIES est conforme au critère. Le mot "impression" est inopportun ici car le modèle centré sur l'utilisateur donne réellement le contrôle à ce dernier. L'aspect "clair et non-ambiguë" est cependant un critère à nuancer, car nous n'avons pas pu nous-mêmes tester l'interface. Par conséquent, nous ne pouvons nous en remettre qu'aux résultats fournis par ARIES. Nous émettons donc des réserves quand au respect d'ARIES envers ce critère.

Expérience cohérente dans tous les contextes :
L'utilisation d'ARIES se fait au moyen d'une application mobile et donc, à fortiori, à l'aide d'un smartphone. Un peu à la manière de certains paiements en ligne qui peuvent se faire au moyen d'un QR code à scanner, ARIES fonctionne de la même manière. L'application permet de dériver l'identité de base en ce qu'ils appellent des identités virtuelles. Il est donc possible de dériver autant d'identités virtuelles qu'il existe de contextes différents. Par conséquent, nous pouvons considérer que le projet ARIES fournit une expérience cohérente dans tous les contextes. Cela signifie qu'ARIES permet aux utilisateurs de se connecter à tous les services qui sont également liés à ARIES au moyen d'une seule application, ce qui implique une expérience homogène d'une utilisation à une autre.

Authenticité de l'identité :
L'authentification dans ARIES se fait sur base de documents physiques (passeport et carte d'identité) émis par des autorités reconnues. Par conséquent, les informations qui en découlent sont authentiques.

Contrôle des autorités :
Le contrôle des autorités est présent sous deux formes pour le projet ARIES. D'une part, et nous rejoignons quelque peu le critère précédent pour cela, les documents sur lesquels se base ARIES pour l'authentification sont émis par des autorités reconnues, ceux-ci apportent une certification quant à l'authenticité de ces documents. D'autre part, le projet inclut un composant appelé le "Secure Vault", pour coffre-fort sécurisé. Ce dernier stocke les logs de toutes les transactions et utilisations d'identités virtuelles anonymisés. En cas de problème dû à la cybercriminalité, les autorités peuvent y avoir accès et ont à disposition des outils pour désanonymiser son contenu à des fins d'investigation. Le projet répond donc favorablement à ce critère.

Sécurisation des données :
La solution d'ARIES est de stocker les éléments d'identités sur le téléphone portable de l'utilisateur, dans le portefeuille sécurisé. C'est un stockage sécurisé, crypté, et protégé par des mesures telles qu'un code PIN, une empreinte digitale ou autres attributs biométriques. Les données qui sont stockées dans le coffre-fort sécurisé sont, elles, cryptées et anonymisées.

5.2.5 Conclusion et pistes d'amélioration

Voici sous forme de grille(11), la synthèse de l'analyse du projet ARIES selon les critères préalablement choisis :

Grille d'analyse - ARIES		
#	Critères	Respect du critère
1	Contrôle et consentement de l'utilisateur	Oui, un consentement explicite est nécessaire pour divulguer des attributs d'identité.
2	Divulgation minimale et usage limité	Oui, les attributs requis sont utilisés, pas plus.
3	Tiers légitimes	Nous émettons quelques réserves pour ce critère. Manque d'avertissement des tiers envers l'utilisateur.
4	Identité dirigée	Nous n'avons pas trouvé d'information à ce sujet.
5	Pluralisme d'opérateurs et de technologies	Oui par design. Autorise plusieurs fournisseurs d'identité non-ARIES, atteignables via protocoles standards (SAML, OAuth,...).
6	Intégration humaine	Par manque de recul, nous émettons des réserves quant à ce critère.
7	Expérience cohérente dans tous les contextes	Oui, peu importe le fournisseur de service, d'un point de vue utilisateur cela se fait toujours via la même interface de l'application mobile.
8	Authenticité de l'identité	Oui de par la nature officielle des documents physiques utilisés comme base.
9	Contrôle des autorités	Oui sous deux formes. Sur base des documents physiques (leur nature officielle) puis via le coffre-fort sécurisé en cas de litige.
10	Sécurisation des données	Oui, via portefeuille sécurisé et coffre-fort sécurisé.

FIGURE 11 – Grille d'analyse - ARIES (vert = ok ; orange = moyen ; rouge = mauvais)

Le projet ARIES est globalement un bon candidat puisqu'il répond favorablement à beaucoup de critères. D'un point de vue purement analytique, au regard de notre grille d'analyse, nous pourrions ainsi imaginer une telle solution déployée à grande échelle. Le projet propose notamment un aspect fort intéressant pour les plateformes de l'économie collaborative : le coffre-fort sécurisé. Ce dernier étant accessible aux autorités en cas le litige, c'est un vrai plus pour rassurer les utilisateurs. De plus, ARIES donne le droit à l'utilisateur de dériver des identités virtuelles de documents d'identité officiels tels le passeport électronique ou la carte d'identité. Son aspect centré sur l'utilisateur donne aussi

plus de contrôle à l'utilisateur à l'égard de ses données d'identité. Le principal problème avec ARIES réside dans la disparité des pays dans leur déploiement d'eIDs. En effet, tous les pays n'en sont pas au même point et tous les eIDs ne sont pas compatibles avec NFC comme en Espagne. Le passeport européen, lui, est compatible mais nombreux sont les citoyens qui ne disposent pas de ce document.

5.3 STORK 2.0

5.3.1 Introduction au projet

Les motivations et ambitions du projet "STORK" (Secure idenTity acrOss boRders linKed) sont définies par (Leitold 2011, p.1)[22] : « Secure means of identification and authentication is key to many services such as in e-government or e-commerce. Several countries have issued national electronic identity (eID) infrastructure to support such services. These initiatives however have often emerged as national islands ; using eID crossborder has not been on the agenda in most cases. This creates electronic barriers ». C'est sur cette base qu'a été lancé le projet STORK dès 2008. Comme le projet précédent, STORK a également bénéficié d'un financement de la commission européenne. Étalé sur 42 mois, le projet STORK devait, à la fin, permettre aux citoyens d'utiliser leur carte d'identité nationale dans n'importe quel pays de l'union européenne. Le but du projet n'était toutefois pas de remplacer les systèmes nationaux eID existants, mais de s'appuyer sur ceux-ci comme base de leur architecture d'identité numérique. Ceci est clairement précisé dans le rapport final du projet[17] : « STORK has not intended to replace any existing national infrastructure, but rather to take what was already available and to connect all the various authentication methods in such a way that any of these methods allow citizens to use their certified personal data with foreign administrations ».

Le projet initial a donné lieu à "STORK 2.0", qui s'est étalé d'avril 2012 à septembre 2015, afin d'apporter des améliorations au projet STORK premier du nom. Les objectifs de STORK 2.0 étaient donc les suivants :

- Accélérer le déploiement de l'eID aux services publics.
- Étendre l'utilisation de l'eID comme cela a été fait pour les citoyens, aux personnes morales ainsi qu'aux petites et moyennes entreprises au sein de l'union européenne.
- Maximiser l'adoption des solutions STORK à travers l'union européenne.
- Tester, dans des conditions réelles, la sécurité et l'utilisabilité des solutions eID dans quatre projets pilotes transfrontaliers.

5.3.2 Statut du projet

STORK fut un succès puisqu'une solution fonctionnelle existait à la fin du projet initial. Toujours selon le rapport final[17] : « The resulting solution, based on a distributed architecture, is robust, transparent, safe to use and scalable, and is implemented in such a way that it is sustainable beyond the life of the

project ». Le projet a même pu tester la plateforme d'interopérabilité à l'échelle de l'union européenne au travers de six projets pilotes qui sont, eux aussi, décrits dans le rapport final du projet STORK[17] :

- **Authentification transfrontalière pour les services électroniques :**
  Le but de ce projet pilote était de permettre aux services des états membres de l'union européenne d'être accessibles de manière sécurisée par les citoyens des autres états membres.
- **SaferChat :**
  SaferChat est une plateforme où les jeunes de quatorze à dix-huit ans peuvent communiquer dans des salons de discussion virtuels. La particularité est que ces jeunes utilisateurs proviennent de différents états membres de l'union européenne et qu'ils doivent utiliser leur carte d'identité nationale pour l'identification, l'authentification et les autorisations.
- **Mobilité étudiante :**
  Ce projet pilote permet aux citoyens européens d'étudier dans des institutions académiques des états membres de l'union européenne, et cela même si elles ne font pas partie de leur état d'origine. Le but était de faciliter la mobilité des étudiants entre pays. Les institutions qui participaient au projet pilote fournissent une panoplie de services en lignes pour les étudiants étrangers tels que : inscription en ligne, librairie virtuelle, traductions, accès à du matériel informatique et aux réseaux ainsi qu'à des cours en lignes et des didacticiels.
- **eDelivery :**
  Une directive européenne stipule que les administrations publiques doivent être capables d'envoyer des documents électroniques aux citoyens et aux prestataires de services. Le projet pilote eDelivery relève le défi de l'identification et de l'authentification de l'identité des destinataires des livraisons électroniques, ainsi que de la manière de rendre les portails de livraison électronique des gouvernements nationaux accessibles aux citoyens de tout État membre.
- **Changement d'adresse :**
  Le projet voulait démontrer qu'il est possible de rendre plus facile la déclaration d'adresse résidentielle pour les citoyens européens lorsqu'ils déménagent d'un état membre à un autre. Les citoyens peuvent alors utiliser leur eID pour se connecter, s'authentifier et modifier leur adresse sans avoir besoin de passer par les administrations publiques.
- **Intégration ECAS :**
  Le but de ce projet pilote était d'intégrer STORK avec l'ECAS (European Commission Authentication Service), ce qui permet aux états membres d'utiliser leur eID nationaux pour fournir une authentification et un accès aux services électroniques fournis par la commission européenne.

Par la suite, le projet STORK 2.0 entreprit de nouveaux projets pilotes afin d'aller plus loin dans la démarche développée par STORK 1.0, et en lui apportant de nouvelles fonctionnalités. Nous décrivons brièvement ci-dessous les projets pilotes menés par STORK 2.0 :

— **eLearning diplômes universitaires :**
L'objectif général de ce projet pilote était de fournir des services transfrontaliers liés au monde académique aux utilisateurs des différents états membres de l'union européenne.
— **eBanking :**
Le but de ce projet pilote était de permettre aux personnes physiques et morales de l'environnement STORK d'utiliser leur identité électronique pour utiliser les services de banques à l'étranger et pour s'authentifier à leur site web.
— **eHealth :**
L'objectif de ce pilote était de porter l'identification et l'authentification des citoyens européens au secteur de la santé.
— **Services publics aux entreprises :**
L'infrastructure STORK 2.0 devait être capable de fournir les services de gestion d'identité nécessaires pour permettre à des personnes et sociétés étrangères (au travers de leur représentant légal) d'accéder aux services en ligne pour les sociétés aussi facilement que ça l'est pour les citoyens nationaux.

Les projets STORK et STORK 2.0 furent de francs succès car ils ont pu démontrer la faisabilité d'une interopérabilité à l'échelle européenne dans des projets pilotes, et pourtant nous n'avons trouvé aucune trace d'implémentation de ces projets, puisque leur déploiement n'a pas été au-delà des projets pilotes.

5.3.3 Fonctionnement et/ou architecture du projet

Le principe fondamental du projet STORK (que ce soit 1.0 ou sa version 2.0), est de réutiliser les systèmes de gestion d'identité (eID) nationaux des états membres de l'union européenne et d'ajouter une couche d'interopérabilité par-dessus ces derniers. Cela afin que les infrastructures existantes dans les différents états membres n'aient pas à être modifiées. Ce projet permet d'éviter le coût qu'engendrerait de devoir conformer tous les états membres à un seul système, surtout pour ceux qui en possèdent déjà un.

Pour parvenir à cela, les membres du projet STORK ont développé deux modèles d'interopérabilité :

— **Modèle "proxy" (fédéré) :**
Cette première approche consiste à déléguer le processus d'authentification. Le fournisseur de service étranger délègue le processus d'authentification à un gestionnaire d'identité du pays d'origine de l'utilisateur. Concrètement, cela peut être représenté par le schéma(12) ci-dessous :

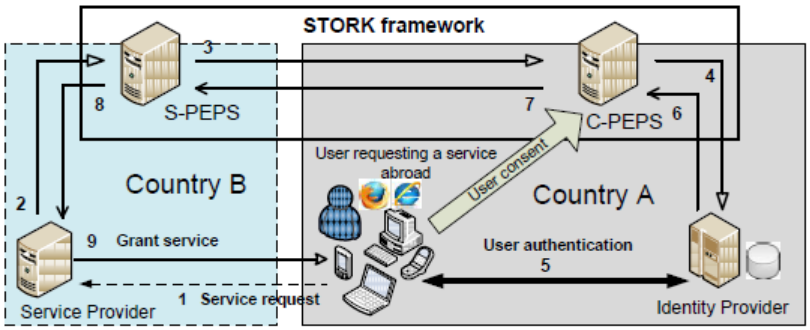

FIGURE 12 – STORK : modèle "proxy" (Berbecaru, Lioy, Mezzalama, Santiano, Venuto, Oreglia 2021, p.6)[12]

Le processus s'effectue alors comme suit :

1. L'utilisateur essaie d'accéder à un service d'un autre pays de l'union européenne. Le fournisseur de service demande alors à l'utilisateur de s'authentifier.
2. Puisque le fournisseur de service est connecté à STORK, il crée une requête d'authentification SAML avec les attributs nécessaires au service et l'envoie au "S-PEPS" (Sp-country Pan-European Proxy Service), qui n'est autre que le service proxy du pays d'origine du fournisseur de service (et de son service) auquel l'utilisateur désire accéder. À cette étape, l'utilisateur doit également préciser son pays d'origine.
3. De là, l'utilisateur est redirigé vers son "C-PEPS" (Citizen-country Pan-European Proxy Service) national. Le S-PEPS construit une requête SAML signée contenant les attributs requis au format STORK et l'envoie au C-PEPS.
4. Le C-PEPS crée une requête d'authentification destinée au fournisseur d'identité national de l'utilisateur, où les attributs nécessaires (reçus au format STORK) sont mappés au format de ce fournisseur d'identité.
5. Le fournisseur d'identité national effectue l'échange d'authentification avec l'utilisateur.
6. Le fournisseur d'identité national renvoie une réponse au C-PEPS suite au processus d'authentification effectué à l'étape 5.

7. Après avoir validé la réponse, le C-PEPS fait correspondre les attributs de la réponse au format STORK, et dérives des attributs supplémentaires si nécessaire. Par exemple, il pourrait créer un attribut "âge supérieur à", dérivé de la date de naissance de l'utilisateur. Le C-PEPS demande également le consentement de l'utilisateur pour transférer ses attributs au S-PEPS, et, le cas échéant, crée une réponse SAML signée et l'envoie au S-PEPS.
8. Le S-PEPS effectue des actions similaires au C-PEPS de l'étape 4, où les attributs reçus au format STORK sont cette fois mappés au format du fournisseur de service étranger, et transmet une nouvelle réponse SAML avec ces attributs au fournisseur de service.
9. Le fournisseur de service extrait les attributs et les vérifie, pour finalement accepter l'accès (ou non) au service désiré.

— **Modèle "middleware" (distribué) :**
Dans cette deuxième approche, l'utilisateur s'authentifie directement auprès du fournisseur de service, au moyen du middleware. Le fournisseur de service reste responsable de la protection des données et a ainsi une responsabilité officielle, puisque cette dernière n'est alors pas transférée à un "tiers" comme dans le modèle fédéré (proxy). Chaque fournisseur de service doit alors intégrer le composant middleware permettant de reconnaître et gérer les eIDs étrangers. L'expérience utilisateur reste ainsi classique et similaire à l'accès à un fournisseur normal, la seule différence étant que la relation est étendue aux utilisateurs des autres états membres de l'union européenne. Cela peut être représenté par le schéma(13) ci-dessous :

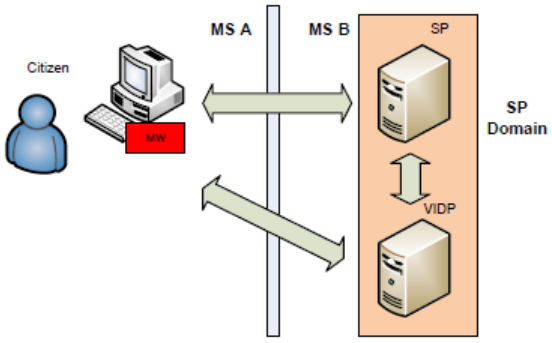

FIGURE 13 – STORK : modèle "middleware" (Leitold, Lioy et Ribeiro 2014, p.3)[23]

Le composant d'interopérabilité est dans ce cas-ci appelé "V-IDP" (pour Virtual Identity Provider). Il est intégré à chaque fournisseur de service implémentant l'approche distribuée et permet de résoudre l'authentification des autres états membres ayant choisi cette approche. Dans le cas où

l'utilisateur doit contacter un état membre ayant opté pour l'approche fédérée, le V-IDP redirige la requête vers le C-PEPS dont nous avons déjà parlé dans l'approche fédérée. Notons que cette redirection n'est pas représentée sur ce schéma(13).

Les deux approches sont elles aussi interopérables l'une avec l'autre puisqu'elles sont basées sur les mêmes protocoles et il est du ressort de chaque pays de choisir l'implémentation qui lui convient. « The MS choices for models are dependent on weighing those pros and cons and on how the national eID is already integrated » (Leitold, Lioy and Ribeiro 2014, p.3)[23]. Par conséquent, un citoyen d'un pays ayant déployé l'approche fédérée pourra quand même utiliser les services de pays ayant opté pour l'approche distribuée, et vice versa.

5.3.4 Analyse sur base de la grille d'analyse

Contrôle et consentement de l'utilisateur :
Ce critère est amplement respecté et ce quelque soit le modèle choisi par les états membres : « Both models take explicit user consent as the basis for legitimacy of data processing and transfer, thus – aside technical measures – establishing consent as the root to data protection compliance » (Leitold 2011, p.6)[22].

Divulgation minimale et usage limité :
Afin d'atténuer les problèmes de confidentialité, l'infrastructure STORK implémente un certain nombre de politiques et d'exigences soutenues par la législation européenne. Un exemple de cela est que les fournisseurs de services ne doivent demander que le minimum nécessaire d'attributs d'un citoyen pour autoriser ou compléter une action donnée. Des attributs de divulgation minimale ont été créés sur base de l'application du respect de la vie privée. Un exemple d'un tel attribut est "âge supérieur à" qui, comme son nom l'indique, permet à un fournisseur de service de demander si le citoyen a un âge supérieur à un âge donné, sans pour autant que le gestionnaire d'identité ait besoin de divulguer l'âge réel du citoyen, mais seulement une valeur booléenne vraie ou fausse dans la réponse (Leitold, Ribeiro, Esposito and Mitzam 2018, p.10)[29]. Il faut également avoir à l'esprit que tous les états membres n'ont pas les mêmes règles pour un même attribut, ainsi : « If some user attributes are prevented by law to be disclosed to foreign service providers, or if they should only be disclosed if specifically agreed by the user, or if an attribute value cannot be disclosed but can be validated then the C-PEPS (and eventually S-PEPS) should enforce it » (Leitold, Ribeiro, Esposito and Mitzam 2018, p.8)[29].

Tiers légitimes :
Ce critère est rempli par l'infrastructure STORK. Que ce soit le modèle fédéré (proxy) ou distribué qui soit déployé. Dans le modèle fédéré, ce n'est pas le fournisseur de service qui est directement responsable de l'authentification de l'utilisateur. Un échange s'effectue entre fournisseurs d'identités nationaux. Par conséquent, l'utilisateur est mis en relation avec des tiers autres que le fournisseur de service initial. Cependant, cela est toujours fait avec le consentement

préalable de l'utilisateur. Par conséquent, ce dernier est averti des tiers contactés lors de la phase d'authentification. Nous pouvons ainsi considérer que le modèle fédéré est conforme. Dans le cadre du modèle distribué (middleware), le problème ne se pose pas puisque le middleware en question est placé, en quelque sorte, sous forme de plug-in chez le fournisseur de service. Le middleware est capable de lui-même d'authentifier les requêtes venant des différents états membres (en ayant la capacité à reconnaître les différents eIDs) directement et par conséquent n'a pas besoin de passer par un tiers.

Identité dirigée :
Une fonctionnalité proposée par STORK, qui améliore la vie privée, consiste à utiliser des pseudonymes par service. « This balances accountability with privacy, as pseudonyms enable the former while still protecting the latter, hence minimizing the risks of identity theft. Pseudonyms are mainly generated by C-PEPS in countries with the centralized model or by the MARS system in distributed model countries » (Leitold, Ribeiro, Esposito and Mitzam 2018, p.10)[29]. Ces pseudonymes sont ainsi des identités omnidirectionnelles, pour reprendre le mot employé par (Cameron 2005)[15]. Tandis que les identités classiques utilisées dans le système STORK sont unidirectionnelles.

Pluralisme d'opérateurs et de technologies :
Ce critère est respecté pour le projet STORK, que le choix se porte vers l'approche fédérée ou distribuée :

- Dans le cadre du modèle fédéré (proxy), c'est le cas puisque le système donne la possibilité aux citoyens européens d'utiliser leur propre eID national pour accéder à un service en ligne étranger mis à disposition par un fournisseur de service connecté à STORK (Berbecaru, Lioy, Mezzalama, Santiano, Venuto, Oreglia 2021, p.7)[12].
- Pour ce qui est de l'approche distribuée (middleware) : Le composant middleware permet un déploiement décentralisé de STORK. Il est déployé à la fois chez les clients et les fournisseurs de services, et doit pouvoir gérer les différents eID étrangers existants, qui peuvent être basés sur différents protocoles et technologies sous-jacentes. Afin de prendre en charge ces exigences, le middleware a une concepption modulaire et extensible de sorte que la prise en charge des différentes technologies eID peut être ajoutée via des modules au composant principal (Leitold, Ribeiro, Esposito and Mitzam 2018, p.8)[29].

Intégration humaine :
Selon (Leitold, Ribeiro, Esposito and Mitzam 2018, p.13)[29] : « STORK cross-border authentication process requires the user to visit a number of different sites, S-PEPS, C-PEPS, IdP. Some of those visits can be made invisible to the user, but others are not. For instance, the user may choose the country of origin in the SP and transmit that information to the S-PEPS, thus allowing the latter to be invisible, but National regulations impose that C-PEPS asks for ex-

plicit consent of the user to send attributes cross-border, and therefore cannot be made invisible. Invisible visits improve the user experience while weakening data-protection guarantees ». Les auteurs nous font part d'une "démultiplication" des sites à visiter pour parvenir à s'authentifier. Il est vrai qu'au regard des étapes que nous avons présentées dans la section dédiée au fonctionnement de STORK, le processus peut s'avérer lourd. Cependant, cela peut être le prix à payer pour une identité authentifiée et une protection des données garanties qui, d'un point de vue "intégration humaine", peut conduire à un basculement d'une confiance décidée à une confiance assurée.

Expérience cohérente dans tous les contextes :
Le projet STORK ne permet pas à l'utilisateur de choisir l'identité à utiliser, car c'est toujours la même, c'est-à-dire son identité telle qu'elle a été délivrée par son pays d'origine. Néanmoins, l'expérience utilisateur, elle, demeurera toujours la même d'un fournisseur de service à un autre et ce malgré les deux modèles qui existent, puisqu'ils sont interopérables. L'expérience utilisateur reste ainsi cohérente et homogène d'un contexte à un autre.

Authenticité de l'identité :
Il n'y a pas vraiment de discussion à avoir concernant ce critère. L'essence même du projet est de fournir une couche d'interopérabilité par-dessus les systèmes de gestion d'identité nationaux, et ces identités nationales sont délivrées par les services gouvernementaux. Chaque identité est forcément unique et authentique dans les systèmes nationaux et c'est sur cette base que se construit le système STORK.

Contrôle des autorités :
Le projet STORK ne propose pas, comme le fait ARIES, un coffre-fort sécurisé contenant des logs exploitables par les autorités en cas de problème (fraudes, cybercriminalité...). Néanmoins, comme ARIES, ce système offre un contrôle -ex-ante- puisqu'il s'appuie sur les identités produites et authentifiées par les autorités nationales.

Sécurisation des données :
La particularité de STORK est qu'il n'y a aucune donnée stockée. L'authentification est à chaque fois exécutée depuis le début. Toutes les communications sont effectuées avec SAML 2.0. La seule chose qui différencie le modèle fédéré du modèle distribué, en terme de sécurité, est l'introduction d'un intermédiaire pour le modèle fédéré, qui joue le rôle de fournisseur d'identité entre le fournisseur de service et l'utilisateur.

5.3.5 Conclusion et pistes d'amélioration

Voici sous forme de grille(14), la synthèse de l'analyse du projet STORK 2.0 selon les critères préalablement choisis :

Grille d'analyse - STORK		
#	Critères	Respect du critère
1	Contrôle et consentement de l'utilisateur	Oui, consentement explicite nécessaire pendant le processus.
2	Divulgation minimale et usage limité	Oui, seulement les attributs nécessaires sont utilisés.
3	Tiers légitimes	Oui car consentement demandé avant de déléguer l'authentification et de transmettre les données.
4	Identité dirigée	Oui, un mécanisme de pseudonyme auto-généré existe.
5	Pluralisme d'opérateurs et de technologies	Oui, le système doit pouvoir supporter différents fournisseurs de services. De plus, le modèle distribué (middleware) doit être capable de gérer différents types de tokens et leur technologie sous-jacente.
6	Intégration humaine	Moyennement. L'utilisateur est redirigé vers plusieurs pages différentes pour accomplir le flux. Flux "lourd" mais sécurisé. De plus, aucun test possible.
7	Expérience cohérente dans tous les contextes	Oui, quelque soit l'approche implémentée par le pays d'origine, il sera toujours possible d'être interopérable avec l'autre approche. D'un contexte à l'autre l'expérience est cohérente et homogène.
8	Authenticité de l'identité	Oui, de par la nature du document sur lequel repose l'authentification (carte d'identité nationale).
9	Contrôle des autorités	Oui, contrôle en amont. Les autorités en effet certifient l'identité d'un individu via l'authenticité du document d'identité fourni. Par contre, pas de contrôle de logs.
10	Sécurisation des données	Oui, aucune donnée stockée et communications sous SAML 2.0.

FIGURE 14 – Grille d'analyse - STORK (vert = ok ; orange = moyen ; rouge = mauvais)

Le projet STORK apparaît être un bon candidat au regard de l'analyse faite sur base de la grille que nous avons définie. Sa force est que, comme ARIES, il s'appuie sur une base d'identité officielle et authentifiée par les autorités nationales, le projet ayant comme objectif de les rendre inter-opérables à l'échelle européenne. C'est par ailleurs l'ambition du projet que de créer une zone européenne d'identité numérique au départ des spécificités des systèmes d'identité nationaux mais aussi des contraintes légales particulières à chaque état membre.

Cette force du projet qui représente une assurance pour les utilisateurs est, par contre, une difficulté pour ceux-ci au niveau de l'utilisabilité du système. En effet, les architectures proposées par STORK (middleware et proxy) qui nécessitent plusieurs étapes à franchir pour s'authentifier ne sont pas centrées sur l'utilisateur, ce qui entraîne une diminution de l'utilisabilité. Enfin l'analyse montre qu'aucun contrôle n'est rendu possible, comme il l'est pour le projet ARIES, puisqu'aucune base de logs n'est officiellement rendue accessible aux autorités.

5.4 OLYMPUS

5.4.1 Introduction au projet

Le projet OLYMPUS, pour "Oblivious identitY Management for Private and User-friendly Services", est un projet qui a démarré en septembre 2018. C'est également un projet qui fait partie du cadre européen HORIZON 2020. Il a par conséquent reçu un financement de ce dernier, avec une contribution avoisinant les 2,5 millions d'euros, pour un budget total d'environ 3,1 millions d'euros. OLYMPUS part du principe qu'à première vue la vie privée et une identification forte ne vont pas de paire, et sont même intrinsèquement contradictoires[3]. En effet, si un utilisateur est fortement identifié durant une transaction, alors sa vie privée est mise en danger. Toutefois, il existe des mécanismes qui permettent de réconcilier les deux, que ce soit en faisant confiance à un fournisseur d'identité en ligne ou en utilisant des mécanismes cryptographiques tels que des identifiants anonymes[3]. La première solution, rendue populaire par des technologies comme SAML, OpenID Connect et Facebook Connect, a le désavantage, selon la page officielle[3] du projet OLYMPUS, de former un point de défaillance unique en termes de vie privée et de sécurité. Pour ce qui est de la seconde solution, le désavantage est que les utilisateurs doivent s'appuyer sur des périphériques de confiance tels que les cartes à puce pour protéger leurs informations d'identification.

L'objectif du projet est de fournir une toute nouvelle approche en offrant une expérience utilisateur proche des fournisseurs d'identité en ligne traditionnels, mais sans leurs inconvénients. OLYMPUS ambitionne d'être le pionnier dans le domaine de la « gestion d'identités distribuées »[3]. Cela consiste à répartir le rôle de fournisseur d'identité entre plusieurs autorités, afin qu'aucune d'entre elles ne puisse traquer ou se faire passer pour leurs utilisateurs. Cela permet aussi de sécuriser les données d'identité, puisque, étant donné que les données sont partagées entre plusieurs entités pour être traitées, parvenir à attaquer l'une d'elles ne servirait à rien. Il faudrait pour être capable de réunir toutes les données d'identité d'un individu ou d'une population réussir une attaque sur toutes les entités en même temps, ce qui est quasi impossible. Le projet a pour but de permettre à ses utilisateurs de conserver des identités non liées à des fournisseurs de services, tout en utilisant un appareil standard ainsi qu'un unique mot de passe ou attribut biométrique.

L'ambition du projet OLYMPUS est d'établir un cadre européen sécurisé et

interopérable de gestion des identités en tirant parti des solutions eID existantes afin de créer un lien fort avec des identités physiques, tout en s'intégrant aux cadres existants pour faciliter son adoption à grande échelle par les fournisseurs de services.

5.4.2 Statut du projet

Le projet n'est pas encore terminé et sa fin est prévue pour le 30 novembre 2021, selon la page officielle[3]. Mais il approche toutefois de son terme et des tests ont déjà pu être réalisés pour deux scénarios d'utilisation. Nous les parcourons ci-après, en nous basant sur les détails du site officiel du projet[6], sur les pages [2] et [1] respectivement :

— **Mobile Driving Licence (mDL) :**
Ce use case a été pensé pour les situations où une identification en face-à-face sécurisée au moyen d'un document d'identité officiel est requis. Par exemple, la vérification de l'âge ou de la nationalité dans un magasin à l'étranger. L'objectif ici est alors de démontrer une divulgation minimale et sélective d'informations personnelles. Avec ce scénario, ils veulent démontrer la possibilité pour un citoyen d'utiliser le permis de conduire (une version électronique du document officiel présente dans le smartphone du citoyen) pour acheter un bien ou un service restreint (comme une bouteille de vin). À la place de divulguer toutes les informations du document en question, l'utilisateur fournit les informations appropriées à propos de son âge, donnant ainsi la preuve qu'il ou elle a l'âge requis. Ce cas peut être représenté par le schéma(15) ci-dessous :

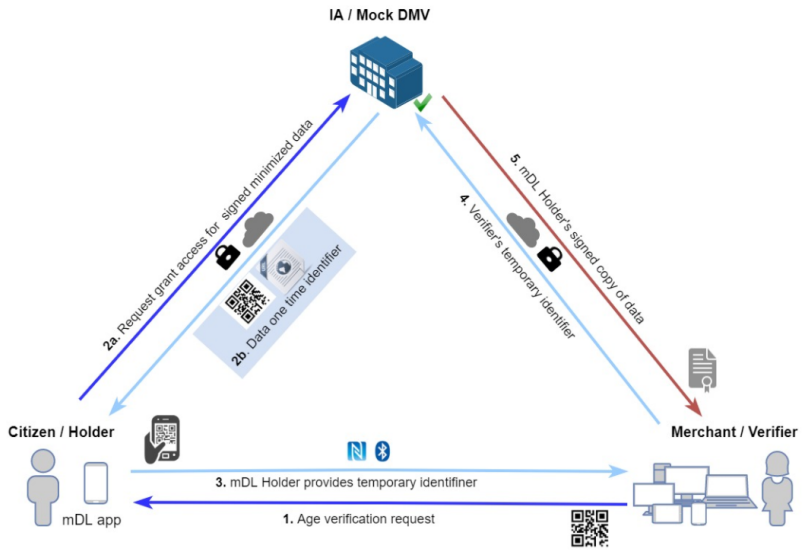

FIGURE 15 – OLYMPUS : Mobile Driving Licence (mDL) use case[2]

Une démonstration de ce cas est également disponible en vidéo[5].

— **Credit File :**
Ce cas a été pensé pour faciliter le processus contractuel lié aux produits et services financiers, tant pour les clients que pour les entités financières. Pour ce cas, une plateforme en ligne est accessible aux petites et moyennes entreprises, les indépendants, les personnes morales ou physiques afin qu'ils puissent gérer leur dossier de crédit. Actuellement, lorsqu'un client a besoin de financement, l'institution financière a besoin de l'identification du client, d'un accès à une base de données externe pour valider les données du client, une évaluation du risque pour le crédit et, s'il est autorisé, d'établir une relation de crédit contractuelle. Depuis les nouvelles règles RGPD, il est nécessaire que le client donne son consentement pour fournir ses données personnelles et qu'il signe un ou des document(s) destinés à être gardé par l'institution financière pendant plusieurs années comme trace du consentement alors que, à ce stade, ni l'institution ni le client ne savent s'ils vont s'engager. Avec OLYMPUS, le processus est facilité pour les deux parties dans le sens où elles ne vont échanger que les données minimales requises avant que le contrat ne soit signé. À la place de recevoir toutes les données d'identification et financières du client à la première étape de la négociation, l'institution financière ne recevra qu'un dossier de crédit anonyme contenant les données financières minimales requises, liées à un pseudonyme, qui permet en premier lieu d'évaluer l'adéquation du client à ce produit ou service spécifique. De là, la banque doit alors produire une réponse basée uniquement sur les données financières du dossier de crédit. Ainsi, la banque ne peut agir avec discrimination sur base du nom, l'indicatif régional ou autre attribut non pertinent. Si elle décide que le client est apte à bénéficier du bien ou du service, le client peut utiliser le pseudonyme pour révéler son identité à la banque, et commencer une relation contractuelle.

Le cas du dossier de crédit peut être représenté par le schéma(16) ci-dessous :

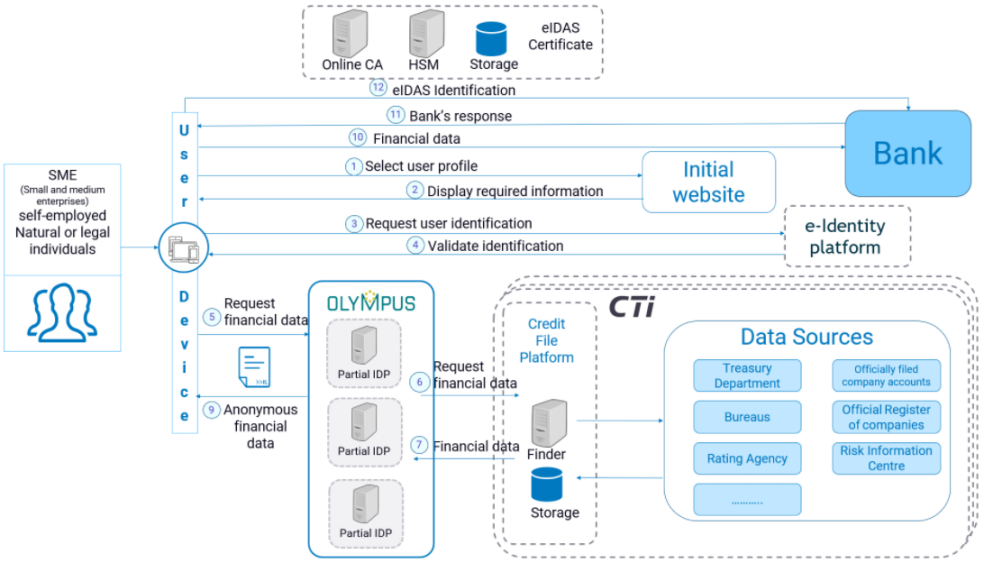

FIGURE 16 – OLYMPUS : Credit File use case[2]

Une démonstration de ce cas est également disponible en vidéo[4].

A ce stade, le projet ne dévoile que deux scénarios d'usage, il faudra voir comment il pourra se comporter dans un déploiement de grande ampleur. Toutefois, l'architecture très distribuée d'OLYMPUS, comme son ambition de diminuer les effets de discrimination ont un potentiel intéressant à explorer dans le cadre de notre problématique de la confiance entre pairs sur des plateformes d'économie collaborative.

5.4.3 Fonctionnement et/ou architecture du projet

Dans l'architecture proposée par OLYMPUS, le rôle de fournisseur d'identité est distribué entre plusieurs entités. Les raisons d'un tel choix sont les suivantes :

— **Sécurité :**
Puisque le travail est réparti entre plusieurs fournisseurs d'identité, il n'est pas possible pour l'un d'eux d'agir malicieusement. Pour mettre en danger le processus, il faudrait que tous les fournisseurs agissent de concert de manière frauduleuse. De la même manière, cette division du travail prévient toute attaque externe. À moins que l'attaquant ne parvienne à contrôler tous les fournisseurs en même temps, il ne sera pas possible pour lui d'usurper le token normalement généré par ces derniers, et donc impossible de se faire passer pour l'utilisateur.

— **Vie privée :**
De par la division du travail entre les différents fournisseurs d'identité, il n'est pas possible pour ces derniers d'identifier la nature et le contenu initial de la transaction car ils ne travaillent que sur une fraction. Par conséquent, ils ne peuvent pas identifier le service auquel l'utilisateur essaie d'avoir accès.

L'infrastructure OLYMPUS peut alors être réprésentée par le schéma(17) ci-dessous :

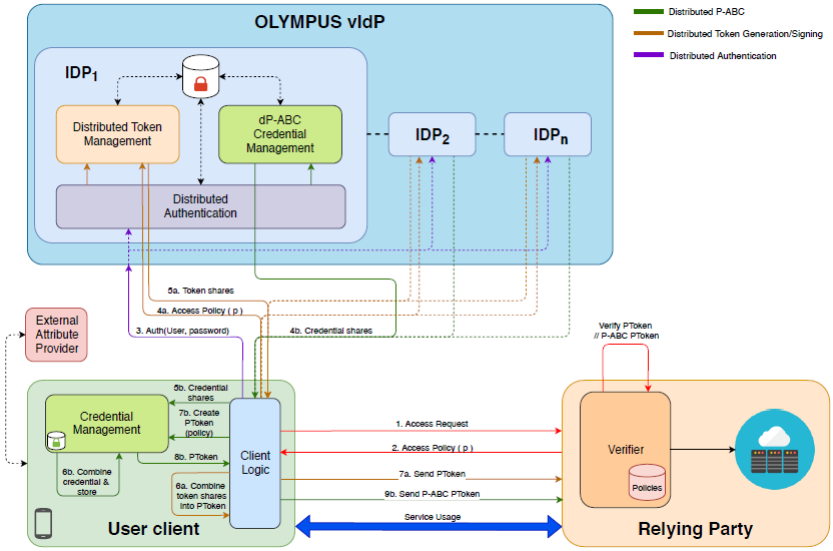

FIGURE 17 – OLYMPUS : architecture (Torres Moreno, Bernal Bernabe, Garcia Rodriguez, Kasper Frederiksen, Stausholm, Martinez, Sakkopoulos, Ponte and Skarmeta 2020, p.7)[32]

Les différents composants du schéma(17) ainsi qu'un flux d'authentification sur base du schéma(17) sont expliqués ci-dessous, comme décrits par les travaux de (Torres Moreno, Garcia Rodriguez, Timon Lopez, Bernal Bernabe and Skarmeta 2020, p.3)[26] et (Torres Moreno, Bernal Bernabe, Garcia Rodriguez, Kasper Frederiksen, Stausholm, Martinez, Sakkopoulos, Ponte and Skarmeta 2020, p.10)[32] respectivement :

— **Virtual Identity Provider (vIdP) :**
C'est le rôle principal de l'architecture proposée par OLYMPUS. Il est rempli par plusieurs fournisseurs d'identité (IDP1, IDP2...IDPn). Ces IDPs proviennent de fournisseurs différents ou sont des entités virtuelles gérées par un même fournisseur. Ils doivent idéalement fonctionner sur des machines physiques différentes, en différents lieux, ne pas avoir le même administrateur système et système d'exploitation (Torres Moreno, Bernal Bernabe, Skarmeta, Stausholm, Kasper Frederiksen, Martinez,

Ponte, Sakkopoulos, Lehmann 2019, p.3)[33]. Cette répartition diminue le risque lié au défaut de fiabilité de l'un des fournisseurs d'identité. Cela par le simple fait que tout seul, un des IDP ne peut être capable de nuire. Chaque IDP implémente un ensemble de modules bien définis, que nous décrivons ici :

- **Distributed Token module :**
  Il est responsable de la génération des fragments de token. Chaque IDP formant le vIdP génère ainsi une partie du token sur base des politiques d'accès données. Quand tous les fragments sont reçus par le client, il est alors en mesure de les combiner pour en faire un token d'accès utilisable auprès du fournisseur de service.
- **Distributed Credential module :**
  Ce module gère la génération d'identifiants ABC (Attribute Based Credentials) de manière distribuée. Comme pour la génération d'un token, chaque IDP génère un fragment et le client est à la fin en mesure de les recomposer. La différence entre cette méthode et la précédente est que celle-ci permet de créer un identifiant ABC, contenant les attributs de l'utilisateur. Cet identifiant n'est pas lié à une politique d'accès et est réutilisable. Il est alors stocké dans l'application mobile OLYMPUS sur le smartphone de l'utilisateur et est réutilisable, notamment pour des scénarios offline. En effet, l'utilisateur sera en mesure de générer des token à présenter au fournisseur de service à partir de ces identifiants, ce qui enlève la nécessité, dans ce scénario, de devoir être connecté aux IDPs. Cela donne notamment la possibilité à l'utilisateur de s'authentifier lors de scénarios "face-à-face" au travers de protocoles à courte portée tels que Bluetooth, NFC,...

Il existe ainsi deux modules distincts au sein des IDPs, et cela reflète les deux méthodes de génération de token/identifiant que supporte l'architecture OLYMPUS.

- **User client :**
  Il définit un composant clé de l'architecture OLYMPUS. Sa première fonction est d'envoyer le nom d'utilisateur et le mot de passe au vIdP pour initier le processus d'authentification distribuée.
  - **Client Logic :**
    Ce module est responsable de la recomposition des fragments de token. Il gère aussi la présentation du token du des identifiants ABC au service auquel l'utilisateur désire accéder. La recomposition des fragments d'identifiants ABC est par contre déléguée au module "Credential Manager".
  - **Credential Manager :**
    Ce module est, lui, responsable de la gestion des identifiants ABC. Il est notamment responsable de la recomposition de ces derniers. C'est également ce composant qui stocke ces identifiants pour des usages ultérieurs. Quand le client désire utiliser l'un de ces identifiants, la politique d'accès est communiquée à ce module et ce dernier génère un token d'accès à présenter au fournisseur de service.

— **Relying Party :**
C'est une entité qui se base sur l'infrastructure OLYMPUS pour générer des politiques d'accès qui doivent être appliquées par les clients dans le but d'accéder à leur(s) service(s). Il faut noter que le client doit donner son consentement pour révéler les attributs nécessaires. Le fournisseur de service joue également le rôle de vérificateur. Il doit ainsi valider le token d'accès fourni par l'utilisateur. Pour effectuer tout cela, deux sous-composants sont nécessaires :
  — **Verifier module :**
  Ce module est en charge de la validation et de la vérification des tokens reçus des utilisateurs. Le processus permet de vérifier que les politiques d'accès sont remplies. Le module gérer n'importe quelle méthode introduite par OLYMPUS (token distribué ou token dérivé d'un identifiant ABC).
  — **Policy DB :**
  Ce module contient l'ensemble des politiques d'accès définies par le fournisseur de service, ce qui définit les attributs spécifiques attendus et requis pour pouvoir faire usage d'un service.
— **External Attribute Provider :**
Enfin, le système OLYMPUS prévoit que les utilisateurs puissent obtenir des attributs provenant d'une source externe. Ce mécanisme peut être précédé d'une vérification de pièce d'identité (par exemple pour les données bancaires). Ainsi, l'utilisateur serait en mesure d'ajouter ces attributs à son profil dans OLYMPUS.

Suivant le schéma(17), un flux d'authentification complet serait le suivant :

1. **Phase d'inscription :**
Cette phase permet à un utilisateur de créer un nouveau compte auprès du fournisseur d'identité distribué (vIdP). Le compte est créé pour un nom d'utilisateur et protégé d'un mot de passe. L'inscription est donc réalisée au moyen de ce nom d'utilisateur, d'un mot de passe et éventuellement d'un ensemble d'attributs. Ces derniers auront été obtenus auprès d'un fournisseur d'attributs externes pour que le vIdP puisse vérifier leur authenticité avant de les accepter et de les stocker. A la fin de la phase d'inscription, l'utilisateur reçoit un message indiquant le succès de l'opération. À partir de ce moment-là, l'utilisateur détient un compte dans le vIdP OLYMPUS.
2. **Phase de génération :**
Cette phase commence quand l'utilisateur veut faire usage d'un service. L'objectif principal de cette phase est d'effectuer l'authentification, la génération et la présentation du token de manière distribuée.
  — **1.** L'utilisateur effectue une demande d'accès à un service auprès d'un fournisseur de service.
  — **2.** Le fournisseur de service transmet alors les politiques d'accès à l'utilisateur, indiquant les attributs requis pour garantir un accès au service.

— **3.** L'utilisateur s'authentifie auprès du vIdP en fournissant son nom d'utilisateur et son mot de passe.
— **4a.** Le module Client Logic du client de l'utilisateur transmet les politiques d'accès aux IDPs du vIdP afin que ceux-ci puissent générer des fragments du futur token d'accès.
— **5a.** Les IDPs envoient leur fragment de token au module Client Logic.
— **6a.** Le module combine tous les fragments générés par les IDPs afin de reconstruire un token d'accès.
— **7a.** Le token d'accès est présenté au fournisseur de service. Ce dernier le vérifie et si tout est correct, autorise l'utilisateur à accéder au service demandé.

———

— **4b.** Chaque IDP du vIdP génère un fragment d'identité ABC, contenant des attributs de l'utilisateur. Les fragments sont envoyés au module Client Logic du composant User Client.
— **5b.** Le module Client Logic n'est pas résponsable de la gestion des identifiants ABC. Il transfère les fragments au module Credential Management du composant User Client.
— **6b.** Le module recombine les fragments et les stocke.
— **7b.** Le module Client Logic demande au module Credential Management de générer un token en fonction des politiques d'accès émises par le fournisseur de service.
— **8b.** Le module Credential Management renvoie le token fraîchement créé au module Client Logic.
— **9b.** Le module Client Logic est maintenant en mesure de présenter le token d'accès au fournisseur de service. Ce dernier vérifie le token reçu et si tout est correct, il autorise l'utilisatuer à accéder au service demandé.

Dans le cas d'un scénario hors connexion, le flux suivrait les étapes dans cet ordre : $1 \rightarrow 2 \rightarrow 7b \rightarrow 8b \rightarrow 9b$.

5.4.4 Analyse sur base de la grille d'analyse

Contrôle et consentement de l'utilisateur :
Comme pour les projets ARIES et STORK, OLYMPUS est conforme à ce sujet puisque le consentement de l'utilisateur est demandé avant toute divulgation d'attribut d'identité, comme le souligne notamment (Torres Moreno, Bernal Bernabe, Garcia Rodriguez, Kasper Frederiksen, Stausholm, Martinez, Sakkopoulos, Ponte and Skarmeta 2020, p.9)[32] : « The user will need to agree the policy and give consent for revealing the attributes ».

Divulgation minimale et usage limité :
Le projet OLYMPUS a comme objectif que le caractère privé des données d'identification ne soit pas altéré. Par conséquent, il vise à ce que le minimum requis soit divulgué. C'est un aspect qui a pu être démontré dans les deux use cases du projet OLYMPUS, le "Credit File" et le "Mobile Driving License", où il était

à chaque fois question de ne divulguer que le strict nécessaire. Ainsi, lorsqu'il faut démontrer que l'on a un âge requis, alors seule cette donnée est utilisée.

Tiers légitimes :
Ce point est délicat pour OLYMPUS puisque nos recherches n'ont pas permis de déterminer si les processus mettent l'utilisateur en garde à propos des tiers faisant partie d'une transaction. Nous avons en effet des doutes quant à ce point puisque le vIdP est un ensemble d'IDPs mais qui nous sont cachés, de par l'abstraction du vIdP. Par conséquent, le token est a priori généré par une boîte noire dans laquelle se trouvent plusieurs fournisseurs d'identité qui travaillent chacun de leur côté pour fournir un fragment de token. Nous considérons ainsi que ce critère n'est pas rempli.

Identité dirigée :
OLYMPUS est conforme à ce critère et cela a été démontré dans le use case du "Credit File". En effet, la première étape consistant à évaluer si un client est apte à contracter un prêt, par exemple, se fait au moyen d'un dossier financier anonymisé, accompagné d'un pseudonyme. Nous voyons en cela une identité omnidirectionnelle, empêchant la banque d'en savoir trop à un moment où elle n'a pas besoin d'en connaître plus sur le client, et ce pour des raisons de discrimination possible dans l'étude d'un crédit, bien identifiées par OLYMPUS. L'identité devient unidirectionnelle lorsque l'utilisateur révèle son identité à l'organisme financier.

Pluralisme d'opérateurs et de technologies :
L'intégration avec des systèmes de gestion d'identité existants est un prérequis au développement de l'architecture OLYMPUS. Par conséquent, le projet est compatible avec SAML, OpenID et OAuth. Cela permet notamment de vérifier les données d'identification apportées par l'utilisateur via le composant "External Attribute Provider". Ce critère est par conséquent rempli.

Intégration humaine :
L'intégration humaine est difficile à cerner puisque nous n'avons pas pu tester l'interface et les flux qu'il est possible de faire. Nous avons pu visualiser des démonstrations officielles ([5] [4]) mais cela ne permet pas de se faire une idée objective et basée sur une expérience réelle d'utilisation. De plus, nous sommes toujours confrontés à ce mécanisme de vIdP pour lequel les démonstrations n'apportent pas plus de réponse quant aux IDPs qui le composent. ([5] [4]). Par conséquent nous émettons des réserves quant à ce critère.

Expérience cohérente dans tous les contextes :
L'utilisation d'OLYMPUS se fait toujours au moyen de l'application et ce pour tous les contextes auxquels l'utilisateur désire accéder. Ce faisant, le projet fournit une expérience homogène d'un contexte à l'autre. Cependant, selon nous,

il ne permet pas de choisir l'identité à utiliser puisque les attributs requis sont définis par la politique d'accès émise par le fournisseur de services.

Authenticité de l'identité :
Comme pour les projets ARIES et STORK, OLYMPUS base les attributs sur des documents officiels authentifiés. Par conséquent, il est certain que les attributs disponibles sont authentiques, de par la nature des documents dont ils proviennent.

Contrôle des autorités :
Le projet OLYMPUS, tout comme STORK, ne propose pas de coffre-fort sécurisé à la manière d'ARIES, contenant des logs exploitables par les autorités en cas de problème (fraude, cybercriminalité,...). Néanmoins, comme les autres, ce système offre un contrôle -ex-ante- de par la nature des documents sur lesquels il s'appuie pour générer des attributs, à savoir les identités produites et authentifiées par les autorités nationales.

Sécurisation des données :
L'authentification auprès du vIdP d'OLYMPUS se fait via un nom d'utilisateur et un mot de passe. Par conséquent, nous pourrions penser que cela est faible d'un point de vue sécurité. Il faut cependant noter qu'il n'y a qu'un seul mot de passe. Par conséquent, l'utilisateur pourra faire l'effort de générer un mot de passe fort puisqu'il n'aura besoin que d'en retenir un seul. Cela contre la tendance qu'ont les utilisateurs à utiliser des mots de passe simples quand ceux-ci commencent à s'accumuler. Aussi, un point fort d'OLYMPUS est la division du travail de génération de token d'accès entre différents IDPs membres du vIdP, puisque cela permet d'augmenter la sécurité (aucun des IDPs n'a l'entièreté des informations), et enlever le point unique d'échec (single point of failure). Par contre, l'abstraction du vIdP est quelque peu inquiétante puisque nous ne savons pas quels sont les IDPs qui le composent (analogie au point "Tiers légitimes"). Par ailleurs, nous ne savons pas de quelle manière un vIdP est choisi pour effectuer l'authentification. Nous n'avons pas trouvé dans nos lectures d'informations permettant d'apporter une réponse claire à cette dernière interrogation.

5.4.5 Conclusion et pistes d'amélioration

Voici sous forme de grille(18), la synthèse de l'analyse du projet OLYMPUS selon les critères préalablement établis :

Grille d'analyse - OLYMPUS		
#	Critères	Respect du critère
1	Contrôle et consentement de l'utilisateur	Oui, consentement explicite de l'utilisateur nécessaire au processus.
2	Divulgation minimale et usage limité	Oui, fortement mis en avant. Uniquement le strict nécessaire est dévoilé.
3	Tiers légitimes	Délicat au regard de la "boîte noire" qu'est le vIdP.
4	Identité dirigée	Oui, système d'anonymisation sous forme de pseudonyme.
5	Pluralisme d'opérateurs et de technologies	Oui, pour pouvoir s'intégrer aux systèmes de gestion d'identité existants. Compatible SAML, OpenID, OAuth.
6	Intégration humaine	Difficile à cerner car aucun test possible.
7	Expérience cohérente dans tous les contextes	Utilisation via application OLYMPUS pour tous les contextes, expérience homogène.
8	Authenticité de l'identité	Comme pour ARIES et STORK, se base sur documents officiels authentifiés.
9	Contrôle des autorités	Oui, contrôle en amont. Les autorités en effet certifient l'identité d'un individu via l'authenticité du document d'identité fourni. Par contre, pas de contrôle de logs.
10	Sécurisation des données	Username et mot de passe unique. Il doit être fort. Aussi, division du travail pour génération du token d'authentification. Réserves à l'égard du vIdP "boîte noire".

FIGURE 18 – Grille d'analyse - OLYMPUS (vert = ok ; orange = moyen ; rouge = mauvais)

Le projet OLYMPUS s'avère être aussi une solution intéressante d'après l'analyse que nous en avons fait, sur base de notre grille et de nos critères. Sa force est la mise à disposition d'une architecture centrée sur l'utilisateur, et d'un aspect sécuritaire très poussé du fait de la division du travail entre plusieurs IDPs rendant a priori impossibles le tracking et le hacking du token. Les plus grosses réserves que nous émettons concernent le vIdP et son effet "boîte

noire". Nous n'avons rien trouvé dans la littérature qui permette d'identifier les différents IDPs d'un vIdP, et les démonstrations vidéo ([5] [4]) ne semblent pas avertir l'utilisateur de l'identité du vIdP séletionné pour une authentification, ce qui implique une entorse au critère "Tiers Légitimes".

5.5 Grille récapitulative

La grille(19) ci-dessous fournit un récapitulatif de l'analyse des trois projets au moyen des critères d'analyse qui avaient été définis :

Grille d'analyse - Synthèse				
#	Critères	ARIES	STORK	OLYMPUS
1	Contrôle et consentement de l'utilisateur	Oui, un consentement explicite est nécessaire pour divulguer des attributs d'identité.	Oui, consentement explicite nécessaire pendant le processus.	Oui, consentement explicite de l'utilisateur nécessaire au processus.
2	Divulgation minimale et usage limité	Oui, les attributs requis sont utilisés, pas plus.	Oui, seulement les attributs nécessaires sont utilisés.	Oui, fortement mis en avant. Uniquement le strict nécessaire est dévoilé.
3	Tiers légitimes	Nous émettons quelques réserves pour ce critère. Manque d'avertissement des tiers envers l'utilisateur.	Oui car consentement demandé avant de déléguer l'authentification et de transmettre les données.	Délicat au regard de la "boîte noire" qu'est le vIdP.
4	Identité dirigée	Nous n'avons pas trouvé d'information à ce sujet.	Oui, un mécanisme de pseudonyme auto-généré existe.	Oui, système d'anonymisation sous forme de pseudonyme.
5	Pluralisme d'opérateurs et de technologies	Oui par design. Autorise plusieurs fournisseurs d'identité non-ARIES, atteignables via protocoles standards (SAML, OAuth,...).	Oui, le système doit pouvoir supporter différents fournisseurs de services. De plus, le modèle distribué (middleware) doit être capable de gérer différents types de tokens et leur technologie sous-jacente.	Oui, pour pouvoir s'intégrer aux systèmes de gestion d'identité existants. Compatible SAML, OpenID, OAuth.
6	Intégration humaine	Par manque de recul, nous émettons des réserves quant à ce critère.	Moyennement. L'utilisateur est redirigé vers plusieurs pages différentes pour accomplir le flux. Flux "lourd" mais sécurisé. De plus, aucun test possible.	Difficile à cerner car aucun test possible.
7	Expérience cohérente dans tous les contextes	Oui, peu importe le fournisseur de service, d'un point de vue utilisateur cela se fait toujours via la même interface de l'application mobile.	Oui, quelque soit l'approche implémentée par le pays d'origine, il sera toujours possible d'être interopérable avec l'autre approche. D'un contexte à l'autre l'expérience est cohérente et homogène.	Utilisation via application OLYMPUS pour tous les contextes, expérience homogène.
8	Authenticité de l'identité	Oui de par la nature officielle des documents physiques utilisés comme base.	Oui, de par la nature du document sur lequel repose l'authentification (carte d'identité nationale).	Comme pour ARIES et STORK, se base sur documents officiels authentifiés.
9	Contrôle des autorités	Oui sous deux formes. Sur base des documents physiques (leur nature officielle) puis via le coffre-fort sécurisé en cas de litige.	Oui, contrôle en amont. Les autorités en effet certifient l'identité d'un individu via l'authenticité du document d'identité fourni. Par contre, pas de contrôle de logs.	Oui, contrôle en amont. Les autorités en effet certifient l'identité d'un individu via l'authenticité du document d'identité fourni. Par contre, pas de contrôle de logs.
10	Sécurisation des données	Oui, via portefeuille sécurisé et coffre-fort sécurisé.	Oui, aucune donnée stockée et communications sous SAML 2.0.	Username et mot de passe unique. Il doit être fort. Aussi, division du travail pour génération du token d'authentification. Réserves à l'égard du vIdP "boîte noire".

FIGURE 19 – Grille d'analyse - Synthèse (vert = ok ; orange = moyen ; rouge = mauvais)

Nous pouvons constater qu'aucun des trois projets analysés ne parvient à répondre favorablement à tous les critères définis. Il y a des informations que nous n'avons pas trouvées dans les rapports produits pour la commission européenne, comme, par exemple, pour le projet ARIES le critère concernant les "Tiers Légitimes". Il y a également un critère assez difficile à évaluer, l'"Intégration Humaine", sur simple base de la lecture des rapports. Toutefois, nous avons pu remarquer que tous ces projets partagent la même ambition, qui est de fournir un écosystème eID interopérable entre tous les pays de l'union européenne. Nous constatons aussi que, dans l'ensemble, ils tentent à rendre possibles les même

types de scénarios. Les trois projets mettent tout en oeuvre pour que le consentement de l'utilisateur soit pris en compte pour la divulgation d'informations d'identité et ils garantissent tous une divulgation minimale de ces dernières, limitée aux attributs strictement nécessaire lors d'un échange donné. Le critère de "Tiers Légitimes" développé par (Cameron 2005, pp7-8) veut que les systèmes de gestion d'identité se conforment au principe selon lequel toute divulgation d'information d'identité soit limitée aux tiers qui en ont un besoin justifié au cours d'une relation d'identité. Selon ce critère, le système candidat doit également avertir l'utilisateur des tiers avec qui il interagit lorsque ce dernier partage des informations. C'est un critère qui, selon nos analyses, n'est pas bien rempli si ce n'est par le projet STORK. En ce qui concerne l'"Identité Dirigée", les projets STORK et OLYMPUS fournissent tous les deux des fonctionnalités à base de pseudonymes permettant à un utilisateur d'être très peu identifiable et à la fois de participer à un processus, comme expliqué dans le scénario du dossier de crédit développé dans le chapitre consacré à OLYMPUS. En ce qui concerne ARIES à l'égard de ce critère, nous n'avons pas été en mesure de trouver les informations permettant de l'analyser. Les trois projets supportent certaines technologies standards comme SAML, OAuth et OpenID afin de s'intégrer au mieux parmi les solutions existantes. Ils s'inscrivent également tous les trois dans une optique de fournir une expérience qui reste cohérente dans tous les contextes. Cela implique que quelque soit le service auquel l'utilisateur désire accéder, les systèmes de gestion d'identité fourniront, chacun à leur manière, une interface offrant une expérience similaire d'un service à un autre. Un point fort que partagent les trois projets est l'authenticité des informations qui sont véhiculées. Cette force réside dans les documents sur lesquels se base les trois projets, à savoir des documents d'identité officiels délivrés par les hautes autorités comme le passeport électronique et la carte d'identité électronique. Dès lors, par cette utilisation de documents officiels, les projets peuvent prétendre à fournir un certain contrôle qui peut rassurer les utilisateurs. Sentiment d'autant plus présent pour les utilisateurs d'ARIES puisque ce dernier offre un contrôle supplémentaire au moyen d'un composant de son architecture, le coffre-fort sécurisé, qui contient les logs de toutes les transactions faites et les preuves des dérivations d'identités. Le tout est anonymisé mais le processus peut être inversé par les autorités à des fins d'investigation en cas de cybercriminalité constatée et plainte déclarée. Le dernier critère de la grille d'évaluation, la "Sécurisation des Données", est assez complexe à analyser, de par les nombreux composants constituant les différentes architectures et les "canaux" de communication qui les relient. Nous nous contentons ici de donner les grandes lignes des éléments utilisés pour garantir la sécurité des données dans les différents projets, qui ont chacun leur manière de faire. ARIES utilise un portefeuille sécurisé à installer sur un smartphone, sous forme d'application. C'est le seul endroit où sont stockées les données d'identification, avec le coffre-fort sécurisé, sous formes d'identités virtuelles dérivées d'une identité physique officielle. Aucun autre composant de l'architecture ARIES ne stocke les données. OLYMPUS utilise sensiblement le même genre de procédé, dans le sens où des identités peuvent être sauvegardées en local dans dans le client (application mobile) afin d'être utilisées lors de scé-

narios hors connexion. Aucun autre composant de l'architecture OLYMPUS ne stocke les données d'identification. La particularité d'OLYMPUS est le processus distribué par lequel le token d'authentification est généré par le vIdP. En effet, chaque IDP faisant partie du vIdP génère un fragment du token et c'est le client utilisateur qui recombine les fragments pour obtenir le token. Cette architecture sécuritaire est un des points forts du projet OLYMPUS souligné par l'ensemble des articles traitant de ce projet. L'intérêt de ce concept est que les IDPs ne sont en aucun cas capables de tracer ou obtenir des données sur l'utilisateur, comme le service auquel il essaie d'accéder par exemple. Nous rappelons toutefois que nous avons émis des réserves concernant le concept de vIdP proposé par OLYMPUS et de son effet "boîte noire". La dernière approche utilisée par STORK est de ne rien stocker. A chaque fois que l'utilisateur désire accéder à un service en ligne au moyen de STORK, il doit alors effectuer le processus d'authentification au moyen de son document d'identité.

En l'état, les projets analysés ont tous démontré qu'ils sont en mesure de permettre aux utilisateurs de se connecter à un service en ligne (comme une plateforme de l'économie collaborative) au moyen d'un document d'identité ou d'une identité dérivée de ce dernier. L'avantage principal de STORK est qu'il permet une interopérabilité des systèmes de gestion d'identité nationaux existant et cela fait de lui la solution qui a sans doute le meilleur potentiel de déploiement à l'échelle européenne. Néanmoins, une piste d'amélioration pour STORK consisterait à améliorer son utilisabilité en rendant les mécanismes opérables au moyen d'appareils mobiles tels que les smartphones.

6 Conclusion

Nous l'avons vu, la confiance est un élément clé de l'économie collaborative car c'est elle qui détermine si nous acceptons de prendre le risque de nous engager dans une transaction ou non. « Lack of trust has been shown to be a major obstacle to the adoption of online shopping » (Chang, Cheung and Tang 2013, p.1)[16]. Nous avons ensuite examiné différents dispositifs de confiance mis en place par les plateformes de l'économie collaborative, à savoir : la réputation (notes et commentaires), les profils utilisateur (description et photo), l'identité digitale (email, téléphone, ID, réseaux sociaux) et les mécanismes indirects (nombre de transactions, nombre de commentaires,...). Sur base d'une revue de la littérature, nous avons pu analyser leurs limites en matière d'établissement d'une confiance entre partenaires d'une transaction. Les limites identifiées sont les suivantes :

- **Réputation :**
  - Non réponse, ne pas effectuer l'évaluation.
  - Avis/note biaisée par peur de représailles.
- **Profils :**
  - **Photos :**
    - Discrimination (raciale,...).
    - Phénomène "beauty premium".

    - Fausse photo, photo trafiquée,...
    - **Informations :** Authenticité des informations non vérifiable.
- **Identité Digitale :**
    - **Email :** Il est trop facile de créer une adresse email anonyme.
    - **ID :** Trop peu répandu.
    - **Réseaux sociaux :** Faux comptes.
- **Mécanismes indirects :**
  Les informations comme le nombre de transactions déjà effectuées ne sont en aucun cas gage de qualité et par conséquent ne peuvent pas à 100% être indicatrices de confiance.

Sur base de cette analyse, il apparaît que le "saut dans l'incertain" que nécessite la réalisation d'une transaction entre pairs se fait essentiellement à travers une sorte de "flair" que développent les utilisateurs à partir de différents indices (photos, commentaires...) sur base desquels ils prennent leurs décisions. Nous sommes dès lors bien dans une "confiance décidée" que (Luhmann 2001, p.12) décrit comme un « (...) calcul purement interne de conditions externes (...) », conséquence directe de l'inefficacité des mécanismes en place actuellement. Partant de ce constat, nous avons voulu dans ce mémoire explorer les systèmes d'identité numérique comme solution possible pour améliorer la construction de la confiance sur les plateformes de l'économie collaborative, et ce, notamment, par l'aspect dissuasif de ces systèmes. Nous supposons en effet qu'il est peu probable qu'une personne ait de mauvaises intentions à l'égard des autres utilisateurs en créant quelque arnaque que ce soit si elle se sait fortement identifiable. Ces systèmes pourraient participer au développement d'une confiance "assurée", pour reprendre les termes de (Luhmann 2001)[25], et alléger le calcul individuel que chacun est obligé de faire aujourd'hui pour "oser" une transaction et, ce, en appuyant ce calcul sur un dispositif de contrôle des identités et de l'authenticité de celles-ci. Les autres mécanismes pourraient alors dévoiler leur plein potentiel même si, toutefois, certains présenteront toujours des biais totalement indépendants d'une identité forte. Sur cette base, nous avons exploré la littérature consacrée aux identités numériques. Celle-ci nous a permis d'une part de comprendre l'ambition de ces systèmes en matière de certification des identités et d'autre part de découvrir différents types d'architectures possibles sur lesquels peuvent reposer ces dispositifs. Cette état de la littérature, nous a également permis d'identifier un projet européen souvent cité en exemple de ces dispositifs, à savoir le projet STORK[8], financé par la commission européenne. Partant de la base des projets financés par la commission, nous avons découvert deux autres projets s'inscrivant dans une proximité d'ambition avec le projet STORK, à savoir les projets ARIES[7] et OLYMPUS[3]. Ce sont ces trois projets que nous avons décidé d'analyser et de comparer afin d'en saisir le potentiel dans la construction d'une confiance assurée pour l'économie collaborative. Au cours de nos recherches, nous nous sommes rendus compte de l'ampleur du travail nécessaire à la bonne compréhension de ceux-ci, étant donné leur complexité. Ainsi, chacun d'entre eux mériterait un mémoire dédié mais nous avons voulu effectuer une première exploration de ces trois projets afin d'en détecter les potentiels respectifs dans leur capacité à restaurer une confiance assurée dans

l'économie collaborative. Pour comparer ces projets, nous avons développé une grille d'analyse s'inspirant des travaux de (Cameron 2005)[15] très centrée sur la protection des données à caractère personnel. Nous avons complété cette grille d'autres critères relatifs à l'authentification des identités, aux rôles des autorités et à la sécurisation des données. L'analyse a montré qu'aucun des trois projets ne permet de répondre favorablement à tous les critères de la grille d'analyse. Il y a également des informations que nous n'avons pas pu trouver. Toutefois, nous avons pu remarquer qu'ils partagent tous la même ambition, à savoir fournir un écosystème eID interopérable à l'échelle européenne, et qu'ils tentent à rendre possible le même genre de scénarios. Les trois projets mettent tout en oeuvre afin que le consentement utilisateur soit au centre de processus, et que les informations divulguées soit minimales et limitées au strict nécessaire. Ils sont également tous les trois compatibles avec des protocoles standards tels que SAML, OAuth,... afin de s'intégrer au mieux aux solutions existantes. Ils fournissent tous, à leur manière, une expérience cohérente et homogène d'un contexte à l'autre. Se basant tous les trois sur des documents d'identité officiels, l'authenticité des identités est alors garantie. En terme de contrôle des autorités, le projet ARIES se démarque en fournissant un coffre-fort sécurisé contenant les logs de toutes les transactions faites et les preuves des identités dérivées, dont le contenu pourra être utilisé par les autorités à des fins d'investigations en cas de cybercriminalité ou de plainte. Du fait d'une analyse qui s'est entièrement basée sur les rapports produits pour la commission européenne, nous n'avons pas pu expérimenter les projets et par conséquent nous ne pouvons statuer sur l'intégration humaine de ces projets. Ce qui les distingue fortement est finalement l'architecture adoptée pour chacun des projets, en termes de composants et de leurs interactions respectives. Les projets ARIES et OLYMPUS sont en effet centrés sur l'utilisateur (user centric), tandis que STORK adopte une approche plus fédérée. Par ailleurs, un des points faibles de STORK est d'être peu centré sur l'utilisateur, alors que ARIES et OLYMPUS le sont. Sur base de ce que nous avons pu lire et analyser, les trois solutions sont, en l'état, déployables et intégrables à des solutions de e-commerce et par conséquent à l'économie collaborative.

Ces projets sont toutefois des projets de recherche et développement. Leurs résultats sont donc des prototypes validés sur différents use cases. Il faudra donc attendre avant de pouvoir conclure à leur faisabilité et leur performance à grande échelle. Il n'empêche que l'émergence d'autant de projets liés à l'identité numérique financés par l'Europe démontre son engouement à développer une confiance assurée sur internet, et, par extension, à promouvoir l'économie collaborative. Cela nous conforte dans notre hypothèse selon laquelle l'identité numérique peut être une solution à notre problématique de construction de la confiance sur les plateformes de l'économie collaborative.

Il se peut que la solution qui sera adoptée à grande échelle ne se basera plus sur le même genre d'architecture que ce que nous avons analysé, car nous commençons à voir émerger des projets relatifs à l'identité numérique utilisant la technologie de la blockchain. Nous avons centré notre analyse sur des projets initiés par la commission européenne. Durant notre travail d'exploration de ces

projets et de revue de la littérature, nos recherches nous ont souvent conduit à des articles traitant de la blockchain, technologie émergente sur laquelle s'appuient de plus en plus de projets liés à l'identité numérique. Il pourrait ainsi être intéressant dans un travail futur d'explorer la blockchain dans son potentiel en matière de sécurisation des transactions et dès lors de construction d'une confiance assurée entre parties dans l'économie collaborative. Ce travail pourrait alors s'appuyer sur celui que nous avons réalisé ici au niveau des identités numériques afin de percevoir les avantages que présentent ces solutions vis-à-vis de celles que nous avons analysées dans ce mémoire.

Nous terminons ainsi ce mémoire en étant convaincus que l'identité numérique deviendra le standard de demain en terme de système de gestion d'identité à utiliser sur internet, ce qui nous permettra de naviguer avec une confiance assurée parmi tous les services que peut offrir le web.

Références

[1] Credit file - olympus. https ://olympus-project.eu/ ?page_id=792. Page consultée le 11 avril 2021.

[2] Mobile driving licence - olympus. https ://olympus-project.eu/ ?page_id=797. Page consultée le 11 avril 2021.

[3] Oblivious identity management for private and user-friendly services. https ://cordis.europa.eu/project/id/786725. Page consultée le 17 mars 2021.

[4] Olympus demonstration of credit file use case. https ://www.youtube.com/watch ?v=8yc7iOo0_Gk. Page consultée le 23 avril 2021.

[5] Olympus demonstration of mdl. https ://www.youtube.com/watch ?v=zBu3jedAi98. Page consultée le 23 avril 2021.

[6] Olympus project. https ://olympus-project.eu/. Page consultée le 11 avril 2021.

[7] Reliable european identity ecosystem. https ://cordis.europa.eu/project/id/700085. Page consultée le 12 mars 2021.

[8] Secure identity across borders linked 2.0. https ://cordis.europa.eu/project/id/297263. Page consultée le 12 février 2021.

[9] An ecosystem to secure our digital identities in the face of rising identity fraud. https ://cordis.europa.eu/article/id/394970-an-ecosystem-to-secure-our-digital-identities-in-the-face-of-rising-identity-fraud/fr. Page consultée le 16 mai 2021, 09 2019.

[10] Bruno Abrahao, Paolo Parigi, Alok Gupta, and Karen Cook. Reputation offsets trust judgments based on social biases among airbnb users. *Proceedings of the National Academy of Sciences*, 114 :201604234, 08 2017.

[11] Paul Belleflamme. *Les plateformes de l'économie collaborative : fonctionnement et enjeux*. 02 2017.

[12] Diana Berbecaru, Antonio Lioy, Marco Mezzalama, Giorgio Santiano, Enrico Venuto, and Marco Oreglia. Federating e-identities across europe, or how to build cross-border e-services. 06 2021.

[13] Jorge Bernal Bernabe, Martin David, Rafael Torres Moreno, Javier Cordero, Sébastien Bahloul, and Antonio Skarmeta. Aries : Evaluation of a reliable and privacy-preserving european identity management framework. *Future Generation Computer Systems*, 102, 08 2019.

[14] Jorge Bernal Bernabe, Rafael Torres Moreno, David Martin, Alberto Crespo, Antonio Skarmeta, Dave Fortune, Juliet Lodge, Tiago Oliveira, Marlos Silva, Stuart Martin, Julian Valero, and Ignacio Alamillo-Domingo. *An Overview on ARIES : Reliable European Identity Ecosystem*, pages 231 – 254. 07 2019.

[15] Kim Cameron. The laws of identity. 11 2005.

[16] Man Chang, Waiman Cheung, and Mincong Tang. Building trust online : Interactions among trust building mechanisms. *Information Management*, 50 :439–445, 11 2013.

[17] Alberto Crespo, Ana Piñuela, and Tony Paradell. Final publishable summary report. https ://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/WP+1+-+Project+Management. Page consultée le 15 avril 2021, 03 2012.

[18] Eyal Ert, Aliza Fleischer, and Nathan Magen. Trust and reputation in the sharing economy : The role of personal photos in airbnb. *Tourism Management*, 55 :62 – 73, 2016.

[19] Faten FARHANI. La sécurité de transaction comme déterminant de la satisfaction et de la confiance électronique du consommateur vis-à-vis d'un site marchand. *Revue Marocaine de Recherche en Management et Marketing*, 0(9-10), 2014.

[20] Walid Hadhri, Laurence Lemoine, and Samy Guesmi. La confiance au cœur des modèles de l'économie collaborative. 06 2017.

[21] Audun Jøsang and Simon Pope. User centric identity management. 01 2005.

[22] Herbert Leitold. Challenges of eid interoperability : The stork project. pages 144–150, 04 2011.

[23] Herbert Leitold, Antonio Lioy, and Carlos Ribeiro. Stork 2.0 : Breaking new grounds on eid and mandates. 11 2014.

[24] Claire Lobet. Confiance et mondes numériques. *Conférence pour l'Université Technique Compiegne*, 09 2018.

[25] Niklas Luhmann. Confiance et familiarité. problèmes et alternatives. *Réseaux*, 108(4) :15 – 35, 2001.

[26] Rafael Torres Moreno, Jesús García Rodríguez, Cristina Timón López, Jorge Bernal Bernabe, and Antonio Skarmeta. Olympus : A distributed privacy-preserving identity management system. pages 1–6, 2020.

[27] Nicolás Notario, Antonio Skarmeta, Jorge Bernal Bernabe, Jose Luis Canovas Sanchez, and Alberto Crespo. Aries : Reliable european identity ecosystem. *ERCIM News*, 04 2017.

[28] Thibault Philippette, Anne-Sophie Collard, and Annabelle Klein. L'économie collaborative : entre jeu, participation et confiance. *Recherches en Communication*, 42 :189–202, 01 2016.

[29] Carlos Ribeiro, Herbert Leitold, Simon Esposito, and David Mitzam. Stork : a real, heterogeneous, large-scale eid management system. *International Journal of Information Security*, 17, 10 2018.

[30] Maarten ter Huurne, Amber Ronteltap, Rense Corten, and Vincent Buskens. Antecedents of trust in the sharing economy : A systematic review. *Journal of Consumer Behaviour*, 16(6) :485–498, 2017.

[31] Timm Teubner and David Dann. How platforms build trust. *SSRN Electronic Journal*, 01 2018.

[32] Rafael Torres Moreno, Jorge Bernal Bernabe, Jesús García, Tore Frederiksen, Michael Stausholm, Noelia Martínez, Evangelos Sakkopoulos, Nuno Ponte, and Antonio Skarmeta. The olympus architecture—oblivious identity management for private user-friendly services. *Sensors*, 20 :945, 02 2020.

[33] Rafael Torres Moreno, Jorge Bernal Bernabe, Antonio Skarmeta, Michael Stausholm, Tore Frederiksen, Noelia Martinez, Nuno Ponte, Evangelos Sakkopoulos, and Anja Lehmann. Olympus : towards oblivious identity management for private and user-friendly services. pages 1–6, 06 2019.

[34] Sung-Byung Yang, Kyungmin Lee, Hanna Lee, and Chulmo Koo. In airbnb we trust : Understanding consumers' trust-attachment building mechanisms in the sharing economy. *International Journal of Hospitality Management*, 83 :198 – 209, 2019.

[35] Georgios Zervas, Davide Prosperio, and John Byers. A first look at online reputation on airbnb, where every stay is above average. 01 2015.